بناء الثّقة: نحو إطار قانوني يحمي البيانات الشخصية في لبنان

دراسة أساسية من إعداد منحة زمالة SMEX لإعداد التقارير عن الحريات الرقمية








www.smex.org

www.facebook.com/smex

www.twitter.com/smex

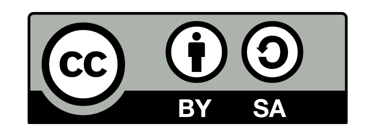


صاحبة زمالة SMEX: إلهام برجس
صاحب زمالة SMEX: حسين مهدي
مديرة التحرير: لارا بيطار
المحرر الاستشاري: محمد نجم

٥ تشرين الأول/أكتوبر، ٢٠١٧

الكتاب: إلهام برجس (كاتبة القسمين الأول والرابع) وحسين مهدي (كاتب القسمين الثاني والثالث)
مساهمة من: سارة رمال، كاتبة مقدمة هذا التقرير والدكتور بيار الخوري، كاتب الخاتمة
المدققة اللغوية: رانيا الغزال
مصمم الجرافيك: www.salamshokor.com

من منشورات عام 2017 لمنظمة SMEX
مبنى قمير، الطابق الرابع، بدارو، بيروت، لبنان.



المحتويات

عن هذا البحث

تمّ إعداد هذا البحث تحت إشراف منحة زمالة SMEX لإعداد التقارير عن الحريات الرقمية.[1]

في لبنان، يتسبّب عدم وجود إطار قانوني شامل للحق في الخصوصية وحماية البيانات بانتهاك الحق في الخصوصية وتنفيذ برامج مراقبة شاملة غير شرعية. لهذا السبب، أطلقت منظمة SMEX في 14 كانون الأول/ديسمبر 2016 تقريرها الإفتتاحي عن المراقبة الرقمية بعنوان "رسم الخريطة لمشهد المراقبة الرقمية في لبنان،" وذلك لفهم الآليات التي تخضع لها المراقبة في لبنان، ولتحديد مجالات الإصلاح السياسي والمناصرة لحماية الخصوصية.[2]

وبعد أن وضعت منظمة SMEX قاعدةً أساسية للمعرفة تتعلّق بالقضايا المرتبطة بالخصوصية، والمراقبة، وحماية البيانات، وجهت دعوة إلى الصحفيين، ونشطاء حقوق الإنسان، والباحثين لإجراء المزيد من التحقيقات حول وضع الخصوصية والمراقبة في لبنان تحت إطار "منحة زمالة SMEX لإعداد التقارير عن الحريات الرقمية."

وقد تمّ تصميم هذا البرنامج من أجل تشجيع، وتسهيل، ونشر الأبحاث حول الحقوق الرقمية في لبنان، وذلك بهدف إحداث تقدّم في المناقشات العامة القائمة على الأدلّة والبراهين. توفر هذه المنحة فرصة تطوير المهارات والخبرة والمعرفة لدى أصحاب الزمالة بشأن قضايا الخصوصية والمراقبة في منطقة الشرق الأوسط وشمال أفريقيا.

الملخص التنفيذي

تسعى الدولة اللبنانية حاليًا إلى الاعتماد بشكل متزايد على التقنيات الرقمية في عملية جمع البيانات الخاصة بالأفراد وتخزينها، وقد سبق أن بدأت بإصدار جوازات السفر البيومترية والإقامات البيومترية الذكية فضلاً عن تحويل دفاتر السوق إلى رخص بيومترية. ومن الواضح أنّ الحكومة تعمل على التوسع أكثر في هذا المجال وذلك عبر اللجوء إلى تقنيات لجمع بيانات إضافية عن الأفراد من خلال شركات خاصة، مثل اقتراح وزير الاتصالات الذي يقضي بالتعاقد مع شركة مختصّة لربط أرقام هواتف الأفراد بهوياتهم. والجدير بالذكر أنّ كل ذلك يجري في ظل عدم وضوح كيفية حماية هذه البيانات وطبيعة النظام الذي تخضع له ومدى حمايته لهذه البيانات وبالتالي حمايته لحق الأفراد في الخصوصية لا سيما مع حدوث حالات تسريب معلومات بات بعضها معروف من قبل اللبنانيين في حين لا يزال البعض الآخر موضع تساؤل.

يستدعي هذا الواقع دراسة الإطار التنظيمي، لا سيما التشريعي، والتقني لمعالجة البيانات الشخصية العائدة إلى المواطنين اللبنانيين وكل مقيم على الأراضي اللبنانية. ستسمح هذه الدراسة بالتالي بتقييم مدى صلابة الإطار الحامي لهذه البيانات أو مدى هشاشته وهشاشة الحقوق المرتبطة به. ويتطلب هذا التقييم إلقاء الضوء على الواقع التشريعي المختص بالبيانات الشخصية في لبنان من جهة، والآليات التقنية المعتمدة من قبل السلطات المعنية لتأمين هذه الحماية من جهة أخرى، بالإضافة إلى تسليط الضوء على مجموعة من الأمثلة الواقعية التي تبرر حجم التساؤلات والتشكيكات في مدى فعالية الأنظمة (القانونية والتقنية) المُتبعة وذلك لما تتضمنه من انتهاكات لخصوصية فئة من الأفراد.

تنطلق هذه الدراسة في قسمها الأول من الواقع القانوني المتعلق بالبيانات الشخصية في لبنان حيث يتضح أن هناك نقص في التشريعات المتخصصة بالبيانات الشخصية في القانون اللبناني، على الرغم من مشاركة لبنان في وضع إرشادات الإسكوا الخاصة بتشريعات حماية البيانات الشخصية منذ عام 2012، إلا أن المشروع اللبناني لم يصدر حتى اللحظة أي تشريع في هذا المجال. وبعد البحث في التعريف القانوني للبيانات الشخصية بشكل عام والمفهوم النظري المتعلق بمعالجتها.

ينتقل التقرير في قسمه الثاني إلى تعريف البيانات البيومترية (أو بيانات المقاييس الحيوية) بشكل خاص، بالإضافة إلى تعريف التقنيات المستخدمة في جمعها، وأبرز الطرق المستخدمة في تشفيرها وحمايتها من أي خرق. تبرز الدراسة أهمية اللجوء إلى التقنية البيومترية في ظل التطور التكنولوجي الذي يُهيمن على عصرنا، بالإضافة إلى أهمية استخدام أفضل وسائل الحماية التقنية التي تضمن عدم تسريب هذه البيانات. وقد جرت هذه الدراسة بالارتكاز على الواقع اللبناني وفي إطار تقييمي له، حيث تمّ تلخيص واقع جوازات السفر والإقامات البيومترية المعتمدة مؤخراً من قبل المديرية العامة للأمن العام، وطبيعة البيانات التي تخزنها السلطات عن اللبنانيين والمقيمين في لبنان، خاصة مع تمتع الأمن العام بحق الولوج إلى هذه البيانات من دون الخضوع لأي قيود تفرضها الجهات القضائية.

في القسم الثالث، تستعرض الدراسة أمثلة واقعية من قطاعات مختلفة تُظهر مدى تمتُّع المواطنين والمقيمين في لبنان بحقهم في الخصوصية وذلك بناءً على الأسلوب المتبع في معالجة بياناتهم الشخصية التي تتعرض للاختراق والتسريب، بسبب ضعف أنظمة الحماية من جهة، والنقص في التشريعات المتخصصة في هذا الموضوع من جهة أخرى.

في القسم الرابع، يتناول البحث مشروع قانون "المعاملات الإلكترونية وحماية البيانات ذات الطابع الشخصي" المعروض للنقاش حاليًا أمام لجنة

فرعية منبثقة عن اللجان النيابية المشتركة. يتضمن هذا المشروع بابًا كاملاً خاصًا بحماية البيانات الشخصية. وبما أن المشروع لم يصبح قانونا نافذاً حتى اللحظة، تسعى الدراسة من جهة إلى البحث عن النصوص المتناثرة بين قوانين مختلفة، والتي ترمي إلى حماية البيانات الشخصية، وتحرص من جهة أخرى على التدقيق في مشروع القانون ومحاولة تقييمه على ضوء تشريعات أجنبية لا سيما القانون الفرنسي الذي استُوحِيَ منه مشروع القانون اللبناني وإرشادات الإسكوا التي يفترض به أن يتطابق معها. هذا بالإضافة إلى الإضاءة على الدور الذي يلعبه مركز المعلوماتية وتكنولوجيا الاتصالات في نقابة المحامين في بيروت لتحسين الواقع الحقوقي لمشروع القانون من خلال المشاركة في النقاشات الدائرة في اللجنة الفرعية.

المقدمة

"من يدعي أنه لا يكترث للحق في الخصوصية لأن ليس لديه ما يخفيه، كمن يدعي أنه لا يكترث للحق في حرية الرأي والتعبير لأن ليس لديه ما يقوله"، هذه مقولة للعميل السابق في وكالة الأمن القومي الأمريكية إدوارد سنودن الذي سرب وثائق كشفت عن برامج تجسس سرية للحكومة الأميركية. فما مدى صحة هذه المقولة في ظل التطورات التكنولوجية الأخيرة التي باتت تطيح بحقوق الإنسان وحرياته الأساسية؟

بعيدًا عن الإطار القانوني ومن منظور اجتماعي بحت، لا بد من تحديد ردة فعل أشخاص ليس لديهم ما يخفونه إذا اقترب منهم غرباء في الشارع كي يسألوهم عن اسمهم وشهرتهم ورقم هاتفهم أو رصيد حسابهم ومدخراتهم. وماذا لو سُئلوا عن الأمكنة التي زاروها أو الأمراض التي يعانون منها أو حالتهم النفسية أو العاطفية أو المادية أو حتى معتقداتهم الدينية؟ إن القدرة على الوصول إلى هذا النوع من المعلومات بسهولة يشكل اعتداءً على الحق في الخصوصية وحرمة البيانات الشخصية، وإلا لماذا قد يرفض الناس مشاركة معلوماتهم الشخصية مع الغرباء، أو تفاصيل حياتهم الشخصية والحميمة مع جيرانهم وزملائهم؟ خلافًا لسلسلة الأسئلة هذه التي يمكن رفض الإجابة عليها، جعلت أنظمة المراقبة حماية معلوماتنا الخاصة والشخصية أكثر صعوبة، حيث خلق جمع البيانات الشخصية ومعالجتها تحديات جديدة في مجال الحق في الخصوصية، ويعود ذلك بشكل جزئيّ إلى أن التشريعات المتخصصة في بعض البلدان تواجه صعوبة في مواكبة هذه التكنولوجيات نظرًا لتطورها السريع، وبالأخص دول العالم الثالث، بما فيها لبنان.

فمع قدرة الدول الكبرى المُصنعة التكنولوجيات الرقمية على الوصول الشامل وغير المقيد لحركة الاتصالات والبيانات الرقمية من دون أدنى اعتبار للسيادات الوطنية ولحقوق الأفراد والجماعات على حد سواء، باتت بيانات الأفراد الشخصية وخصوصيتهم عرضة للعديد من التهديدات والتعديات. وكل ذلك بحجة الحفاظ على الأمن ومكافحة الإرهاب ومواجهة أنواع الجرائم المختلفة والجرائم المنظمة التي تمارس على شبكة الإنترنت و/أو خارجها. وينطبق ذلك على لبنان، الذي استورد برامج المراقبة الجماعية غير الشرعية.

أدى غياب المنظومة التشريعية المواكبة للتطورات التكنولوجية إلى إعاقة القدرة على حماية بيانات الأفراد من الممارسات التعسفية وغير القانونية، الّتي قد تمارسها جهات فاعلة حكومية أو غير حكومية. وفي العديد من الأحيان، تمكّن مراقبة البيانات الشخصية التي يتم تبادلها عبر الوسائط الرقمية، من رسم صورة واضحة للأفراد وتحركاتهم وطبيعة تواصلهم وعلاقاتهم. لهذا السبب، جمع البيانات الشخصية غير المضبوط، لا يقيد حق الأفراد بالتعبير عن أنفسهم وإيصال آرائهم بحرّية ودونما خوفٍ من مواجهة الإدانة فحسب، إنّما يخرق أيضاً حقّ الخصوصية، إذ تتعّرض بياناتهم، تحرّكاتهم، أو رسائلهم للاعتراض، والتجميع والتحليل وفي بعض الأحيان للاستغلال من قبل هيئات حكومية، مؤسّسات، وشركات خاصة. تحقيق التوازن بين الحقّ بالوصول ومشاركة المعلومات من جهة، وحقّ الخصوصية وحماية البيانات الشخصية من جهة أخرى، هو مشروع ضروريّ لا تعالجه مسودّة قرار البيانات الشخصية الحالية بشكلٍ كاف.

ونظرًا لترابط الحقوق ببعضها البعض، ولأن إعاقة ممارسة أحدها قد يشكّل خطراً على الحقوق الأخرى، يُعتبر هذا التقرير الخطوة الأولى في دراسة الإطار القانوني اللبناني المتعلق بحماية البيانات الشخصية في ضوء المواد الدستورية ومختلف المواثيق الدولية الملزمة للدولة اللبنانية انطلاقاً من الأحكام القانونية المبعثرة في أكثر من قانون (لاسيما قانون العقوبات، قانون السرية المصرفية، قانون الآداب الطبية، قانون حماية المستهلك، قانون أصول المحاكمات الجزائية، الخ)، ووصولاً الى القانون رقم 140/1999 المتعلق بصون سرية المخابرات، الداخلية والخارجية، التي تمارس بكافة وسائل الاتصال، سواء السلكية أو اللاسلكية (الهواتف الأرضية والمحمولة، بما في ذلك الهاتف، والفاكس، والبريد الالكتروني،إالخ)، من خلال استعراض الإطار القانوني الحالي، تهدف هذه الدراسة إلى مساعدة الإصلاحات القانونية، تحديداً تلك الّتي تعالج أهمية حماية البيانات الشخصية، على التقدّم.

القسم الأول: الإطار القانوني

لم يقترح التشريع اللبناني حتى اللحظة أي تعريف لـ "البيانات الشخصية" و"معالجة البيانات الشخصية (أو ذات الطابع الشخصي)" إلى ذلك، لم يولِ لبنان اهتمامًا خاصًا على الصعيد التشريعي بحماية البيانات الشخصية. ولم تبدأ اللجنة المنبثقة عن اللجان النيابية المشتركة سوى مؤخرًا بمناقشة مشروع قانون "المعاملات الإلكترونية وحماية البيانات الشخصية". وقد تمّ تخصيص الباب الخامس من المشروع بكامله لمسألة حماية "البيانات الشخصية."

• تعريف البيانات الشخصية ومعنى المعالجة

تستوحي معظم التشريعات المتعلقة بالبيانات الشخصية تعريفها لهذه البيانات من الاتفاقية الأوروبية لحماية البيانات الشخصية. ويتضمن مشروع القانون السابق الذكر، تعريفًا مستوحى من القانون الفرنسي وهو يمتثل بدوره لما ورد في الاتفاقية الأوروبية. أما في ما يتعلّق بمفهوم معالجة البيانات والضوابط التي يحددها القانون، تتقلّص نسبة التطابق بين مشروع القانون اللبناني والمعايير الدولية.

يُعرّف مشروع القانون اللبناني البيانات الشخصية على أنها "جميع أنواع المعلومات المتعلقة بشخص طبيعي التي يمكن أن تمكّن من التعريف به، على نحو مباشر أو غير مباشر، بما في ذلك عن طريق مقارنة المعلومات المتعددة المصادر أو التقاطع في ما بينها". يتطابق هذا التعريف مع النص الفرنسي، لا سيما أن مشروع القانون اللبناني يستوحي الكثير من أحكامه من القانون الفرنسي حين يتعلق الأمر بالبيانات الشخصية[4].

بشكل عام، تتشابه تعريفات البيانات الشخصية في مختلف القوانين. مثلاً تعتمد الاتفاقية الإفريقية للأمن السيبراني وحماية البيانات الشخصية التعريف نفسه. ويعود هذا التشابه إلى اتخاذ هذه النصوص الاتفاقية الأوروبية لحماية البيانات الشخصية كمرجع لها في هذا المجال.

وقد عرّفت الاتفاقية الأوروبية "البيانات الشخصية" على أنها "كل المعلومات المتعلقة بشخص طبيعي مُعرّف أو قابل للتعرّف عليه". ثم أضيف، بموجب القرار التوجيهي رقم 2008/977 الصادر عن الاتحاد الأوروبي عام 2008 والمرتبط بـ"حماية البيانات الشخصية ضمن الإطار الأمني والقضائي في المجال الجزائي"، إلى التعريف الوارد في الاتفاقية ما مفاده أنها "البيانات التي تتعلق بهوية الشخص البدنية، والفيزيولوجية، والنفسية، والاقتصادية، والثقافية، والاجتماعية."

بناءً على ما تقدم، لا بدّ لأي اقتراح يتناول تعريف البيانات الشخصية أن يأخذ بعين الاعتبار التعريف الأوسع والأشمل المعتمد على الصعيد الدولي. وذلك لأن التشريع يهدف إلى حماية البيانات الشخصية، لا سيما أن كل ما يتعلق بالتكنولوجيا الرقمية يكون دوليًا بطبيعته. وعليه، فإن البيانات الشخصية هي:

> جميع أنواع المعلومات المتعلقة بشخص طبيعي، التي تمكن من التعريف به، على نحو مباشر أو غير مباشر، بما في ذلك عن طريق مقارنة المعلومات المتعددة المصادر أو التقاطع في ما بينها (وفقًا لمشروع قانون المعاملات الإلكترونية)، والتي تتعلق بهوية الشخص البدنية، والفيزيولوجية، والنفسية، والاقتصادية، والثقافية، والاجتماعية.

يتطابق هذا التعريف مع إرشادات لجنة الأمم المتحدة الاقتصادية والاجتماعية لغرب آسيا (إسكوا) للتشريعات السيبرانية، الصادرة عام 2012 في بيروت في إطار مشروع "تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية[5]."

تُعدّ معالجة البيانات الشخصية من أكثر العمليات التي تهدد أمن هذه البيانات. لذا تشكل هذه العملية مسألة محورية بالنسبة للتشريعات المعنية بحماية هذه البيانات. من هذا المنطلق، يعبر التعريف الذي يعتمده أي تشريع في هذا المجال عن مدى تمسكه بتأمين أوسع نطاق من الحماية لهذه البيانات.

يعرّف مشروع قانون المعاملات الإلكترونية والبيانات الشخصية "معالجة البيانات" على أنها "كل عملية أو مجموعة عمليات تقع على هذه البيانات مهما كانت الوسيلة المستخدمة، لا سيما عمليات الجمع والتسجيل والحفظ والتكييف والتعديل والاقتطاع والاستعمال والنقل والنشر والمحو والإتلاف وكل شكل آخر لوضع المعلومات تحت التصرف." لا يُطابق هذا التعريف القانون الفرنسي[3] وحسب، بل يمتثل أيضًا لإرشادات الإسكوا.

يتضمن كلٌّ من النص اللبناني والفرنسي تعريفًا لـ "المسؤول عن معالجة البيانات الشخصية" وآخرَ عن "المرسل اليه البيانات الشخصية". وتجدر الإشارة إلى أن النص الفرنسي يبدو أكثر تفصيلاً، غير أن ذلك لا يؤثر على تطابق النصين. وفقًا لمشروع القانون اللبناني يمكن تعريف الجهتين على الشكل التالي: "المسؤول عن معالجة البيانات الشخصية، هو الشخص أو السلطة العامة أو الهيئة التي تحدد أهداف المعالجة وأساليبها."

أما المشرع الفرنسي فلم يكتفِ بعبارتي "الشخص الطبيعي أو المعنوي"، بل عدد الجهات التي يمكن أن تخضع للقانون بصفتها معالج للبيانات،

وهي: "الأشخاص، أو السلطة العامة، أو الهيئة التي تحدد أهداف المعالجة وأساليبها."

أما المرسل إليه البيانات الشخصية فهو الشخص المخول استلام البيانات الشخصية، وهو غير الشخص المعني بالمعالجة أو المسؤول عن المعالجة أو من ينجزها. ولا تعتبر بحكم المرسل إليه السلطات العامة المخولة قانونًا، ضمن مهمة خاصة، طلب بيانات ذات طابع شخصي.

• كيفية حماية القانون اللبناني للبيانات الشخصية

على صعيد القوانين النافذة في لبنان، لا يوجد حاليًا ضمانات تتعلق بحماية البيانات الشخصية، سوى في بعض النصوص المتناثرة بين القوانين. على الرغم من ذلك، فإن الدولة تتجه أكثر فأكثر إلى جمع هذه البيانات ومعالجتها. وهي تلجأ في هذا الإطار إلى التعاقد مع شركات خاصة محلية وأجنبية، ما يجعل سرية هذه البيانات، وتبعاً حق الأفراد بخصوصيتهم، شديدة الهشاشة.
يتضمن التشريع اللبناني العديد من النصوص المتصلة بأمن المعلومات، أو ما يعرف بـ"أمن الفضاء السيبراني". وهي تحمي بمعظمها حق الأفراد بخصوصيتهم من خلال حماية الجهة المعنية بكل قانون لسرّية بياناتهم. بالمقابل، تتطرق قلّة قليلة من هذه النصوص إلى الحقوق الأخرى، غير الحق في الخصوصية، والتي ترتبط مباشرةً بالبيانات الشخصية.

القوانين اللبنانية التي تعنى بحماية البيانات الشخصية

1- قانون الحق في الوصول إلى المعلومات
تكرس المادتان 4 و5 من قانون الحق في الوصول إلى المعلومات حق الأفراد في الاطلاع على البيانات التي تم جمعها عنهم من قبل الإدارة أو أي من الجهات التي تخضع لأحكام القانون المذكور.
فوفق المادة 4، "يحق لصاحب العلاقة دون سواه الوصول إلى الملفات الشخصية وأي تقرير تقييمي يتعلق بشخص طبيعي مشار إليه بالاسم أو برقم تعريفي أو برمز أو بأي وصف تعريفي آخر كبصمات الأصابع أو العين أو الصوت أو الصورة."

"يُعنى بالملفات الشخصية قيود الأحوال الشخصية والملفات التي تتضمن جميع أنواع المعلومات المتعلقة بالشخص الطبيعي بشكل مباشر أو غير مباشر، بما في ذلك عنوان بروتوكول الإنترنت عن طريق مقارنة المعلومات المتعددة المصادر أو التقاطع في ما بينها."
"ويحق لصاحب العلاقة طلب تصحيح أو إكمال أو تحديث أو محو المعلومات الشخصية المتعلقة به في حال كانت غير صحيحة أو ناقصة أو ملتبسة أو قديمة أو تلك التي يُمنع جمعها أو استعمالها أو تبادلها أو حفظها."
أما المادة 5 فتستثني من المادة السابقة مجموعة من المعلومات، من بينها حياة الأفراد الخاصة وصحتهم العقلية والجسدية والأسرار التي يحميها القانون كالسّر المهني أو السر التجاري.

2- قانون حماية المستهلك (المادة 58)
يلزم هذا القانون الحرفي (أي التاجر أو الصناعي أو صاحب الحرفة أو مقدم الخدمة) بالحفاظ على المعلومات التي يستحصل عليها ولا يتصرف بها ما لم يوافق المستهلك صراحة على ذلك. يتقدم هذا القانون على قانون تنظيم مهنة الطب باشتراطه على الحرفي "اتخاذ كافة الإجراءات للحفاظ على سرية هذه المعلومات". هذا وتخضع أحكام هذا القانون الى محكمة خاصة هي لجنة حماية المستهلك[7]. تتبع هذه اللجنة إجراءات مختصرة، وتعفي المتقدم بالمراجعة أمامها من شرط تعيين محام. كما تتيح لجمعيات المجتمع المدني بالتقدم أمامها بدعاوى إبطال بنود تعسفية تُدرجها الشركات في عقودها. وهذا ما يسمح لهذه الجمعيات بالتقدم بدعاوى ضد أي بند يتيح لشركة ما التصرف بالبيانات الشخصية للأفراد من دون موافقتهم المسبقة، مثلاً. بالتالي تم إحراز تقدم إضافي على صعيد حماية البيانات الشخصية، إلى حين إقرار تشريع مختص في هذا المجال.

3- قرارات وقواعد تنظيمية وتعاميم صادرة عام 2000 عن مصرف لبنان، تتعلق بحماية بيانات الأفراد
نذكر منها على سبيل المثال التعميم رقم 134 بتاريخ 12 شباط/فبراير 2015: "حماية المعلومات المالية والشخصية للعملاء بما لا يتعارض مع التشريعات النافذة لا سيما قانون سرية المصارف وقانون مكافحة تبييض الأموال وتمويل الإرهاب". والقرار رقم 7548 الصادر في 30 آذار/مارس 2000 والمتعلق بالمعاملات المالية والمصرفية بالوسائل الإلكترونية، حيث ينص في المادة 12 منه أنه "بغية الحصول على ترخيص من مصرف لبنان للقيام بعمليات التحويل النقدية بالوسائل الإلكترونية يجب أن تتقدم بطلب مرفق بـ (...) المستندات المتعلقة بأنظمة العمل وبالقواعد التقنية التي ستتبعها في تنفيذ عملياتها الإلكترونية والتي تثبت أن لديها نظام حماية إلكتروني فعال للعمليات التي تجريها..."

القوانين اللبنانية التي تعنى بالحق في الخصوصية

1- قانون التنصت، وهو ينظم عمليات اعتراض الاتصالات ومراقبتها[8].

2- قانون الاتصالات يفرض موجب السرية على كل من يعمل في التفتيش والمراقبة في إطار قطاع الاتصالات (المادة 38)[9].وتنص المادة على أن:

"(...) للمراقب أو المفتش أثناء قيامه بالمهام المكلف بها رسميًا وكلما تطلب تنفيذ المهمة ذلك، دخول جميع الأماكن العامة أو الخاصة، ومعاينة أو طلب أي معلومات عن الإنشاءات والتجهيزات القائمة أو التي كان من الواجب إقامتها، والاطلاع على السجلات والوثائق والمستندات وله أن يأخذ نسخًا أو مقتطفات عنها، وأن يطلب إبراز أي مستند أو تقديم أي معلومات يراها مفيدة. تطبق في حالات الدخول عنوة وتنظيم محاضر ضبط عند وجود أدلة ترجح حصول مخالفة الأحكام المنصوص عليها في قانون أصول المحاكمات الجزائية وكذلك الأصول المتبعة لعمل الضابطة العدلية."
تعتبر المعلومات التي يطلع عليها المراقبون والمفتشون في معرض تنفيذهم لمهامهم سرية ولا يجوز لهم البوح بها إلا أمام رؤسائهم التسلسليين أو بناءً على طلب المرجع القضائي المختص. كما تطبق أحكام السرية على كل من يطلّع على هذه المعلومات بحكم عمله في الهيئة أو الوزارة.

3- قانون السرية المصرفية بموجب قانون 3 أيلول/سبتمبر 1956، الذي تلتزم بموجبه المصارف بالامتناع عن كشف السر المصرفي سواء في مواجهة الجهات الخاصة أو السلطات العامة، وسواء كانت قضائية أو إدارية أو مالية باستثناء حالات محددة حصرًا في القانون.

4- قانون العقوبات اللبناني (المواد 579 – 580 581-) يعاقب "من كان بحكم وضعه أو وظيفته أو فنّه، على علم بسر وأفشاه من دون سبب شرعي..."

وتجدر الملاحظة هنا أن السبب الشرعي قد يعود إلى أوامر تلقاها الموظف من رئيسه التسلسلي. الأمر الذي يؤدي إلى إفلات الموظف من العقاب في ظل غياب نظام واضح يحدد من هي الجهات التي يحق لها الاطلاع على بيانات الأفراد وطلبها. إلى ذلك، فإن هذه المواد تتعلق بالأشخاص الملحقين بوزارة البريد أو الإتصالات الذين يسيئون استخدام صلاحياتهم فينتهكون سرية بيانات الأفراد المستفيدين من خدمات هذه الدوائر. والجدير بالذكر أن هذه المواد ترتبط بصياغتها ومضمونها بأساليب المراسلات بشكلها التقليدي ما قبل الإلكتروني. بالتالي، فإنها لا تواكب هذا التطور. ولكي تكون فعالة في عصرنا هذا، فهي بحاجة إلى اجتهاد قضائي متقدم يعيد تفسير النصوص القانونية بما يتلاءم وعصرها.

5- قانون الآداب الطبية (المادتان 6 و44)
تلزم المادة 6 الطبيب بأن "يحافظ على السر المهني باستثناء ما هو منصوص عليه بالقانون". أما المادة 44 فهي تتعلق بواجب الطبيب المكلف بالمراقبة الطبية من قبل إدارة ما، أن "يحتفظ بسر المهنة ويكتفي بإعطاء معلومات لها علاقة أو فائدة من الناحية الإدارية من دون أن يبين الأسباب الطبية لذلك. وأنه ممنوع من إعطاء المعلومات الطبية المدونة في الملفات الطبية إلى أي أشخاص آخرين أو أي إدارة أخرى، ما عدا الحالات التي تنص عليها القوانين العامة."
تشكل هذه المادة ضمانة قانونية صلبة في ما يتعلق بالمعلومات الطبية الخاصة بالأفراد. غير أنها تبقى غير كافية وحدها في ظل التطور التكنولوجي الحالي الذي يستدعي إلزام المستشفيات والأطباء بتطبيق معايير واضحة لحماية ملفات مرضاهم من أي اختراق إلكتروني ممكن. ويتحمل الأطباء والمستشفيات مسؤولية تسرب بيانات مرضاهم في حال عدم التزامهم بهذه المعايير. ولا بد أن يكون لنقابة الأطباء الدور الأساسي والسباق في هذا المجال.

النصوص الدولية الملزمة للدولة اللبنانية

حتى هذا التاريخ، لم يوقع لبنان على أي اتفاقية دولية تتعلق بحماية البيانات الشخصية. بالتالي فإن الدولة اللبنانية، لا تلتزم على الصعيد الدولي إلا بالمبادئ العامة المكرسة في مجال حماية البيانات الشخصية. وتتضمن قرارات الأمم المتحدة أهمّ هذه المبادئ إذ ينصّ الدستور اللبناني على التزام لبنان بمواثيق الأمم المتحدة والإعلان العالمي لحقوق الإنسان.

تندرج حماية البيانات الشخصية ضمن قرارات الأمم المتحدة المتعلقة بالحق في الخصوصية، وأبرزها قرار الجمعية العامة رقم 86/167. بالتالي، من خلال مشاركة لبنان في رعاية قرار الجمعية العامة للأمم المتحدة المذكور، بالإضافة إلى القرار 166/69 الذي اعتُمد في كانون الأول/ديسمبر 2014، وهو يلتزم بتعزيز، واحترام، وضمان الحق في الخصوصية كحق من حقوق الإنسان.[10]

أما على الصعيد الإقليمي، يعمل المركز العربي للبحوث القانونية والقضائية على تطوير مسودة لاتفاقية عربية تهدف الى "بناء الثقة في الفضاء السيبراني"[11] حيث خصص فيها بابًا لـ"حماية البيانات الشخصية". سيؤدي إقرار هذه الاتفاقية من قبل جامعة الدول العربية إلى خلق إطار قانوني لحماية البيانات الشخصية على صعيد المنطقة العربية. وتتوافق هذه الخطوة مع الاتجاه الدولي في وضع تشريعات دولية في هذا المجال تماشيًا مع طبيعة الفضاء السيبراني العابر للحدود.

بالمقابل، تلتزم الدولة اللبنانية بمجموعة من الاتفاقيات الإقليمية ذات الطابع الأمني، تجعل مسألة حماية البيانات الشخصية، وبالتالي وضع أصحابها، أكثر هشاشة، وذلك لأن الالتزام بهذا النوع من الاتفاقيات لا يقابله أي تشريع داخلي لحماية هذه البيانات وتنظيمها ونقلها ومعالجتها. ومن أبرز هذه الاتفاقيات، الاتفاقية العربية لمكافحة الإرهاب التي انضم اليها لبنان عام 1999، بموجب القانون رقم 57 بتاريخ 31 آذار/مارس 1999،[12] والتي تتضمن نصوصًا تحث الدول المتعاقدة على إنشاء قواعد بيانات، وتبادل المعلومات في ما بينها في ما يختص بكل ما تعتبره مرتبطًا بمكافحة الإرهاب. وقد يؤدي ذلك إلى ملاحقة الأفراد واضطهادهم على خلفية آرائهم السياسية.

باختصار، يضم القانون اللبناني سلسلة من النصوص المبعثرة التي تؤمن حماية بيانات الأفراد ضمن مجموعة من القطاعات. بالمقابل، لا يتضمن التشريع اللبناني أي نص متخصص يتناول مسألة حماية هذه البيانات في إطارها الواسع. يستمر هذا النقص التشريعي في ظل مجموعة من العوامل، لا سيما الأمنية منها وتلك المرتبطة بمكافحة الإرهاب، والتي تتحول إلى ذريعة لخرق بيانات الأفراد وانتهاك حقهم في الخصوصية. وإن كانت هذه الآلية ضرورية لاستباق العمليات الإرهابية، إلا أنها عادةً ما تُستخدم أيضًا للتضييق على الأفراد بشكل عام وعلى الناشطين في مجالات حقوق الإنسان[13] بشكل خاص، وذلك بحجة الحفاظ على الأمن. وهذا ما يضاعف الحاجة إلى الإسراع بإقرار قانون لتنظيم معالجة البيانات الشخصية وحمايتها.

القسم الثاني: أحدث تقنية رقمية متبعة من قبل السلطات اللبنانية — البيانات البيومترية

• تعريف البيانات البيومترية

البيومترية أو المقاييس الحيوية: مصطلح مشتق من الكلمة الإغريقية Biometrics (كلمة Bio ترمز للحياة وكلمة Motron أو metric ترمز إلى القياس)[14].

علم المقاييس الحيوية هو علم التحقق التلقائي من هوية الإنسان عن طريق مكونات الأجسام البشرية، أي من خلال قياس التحليل الإحصائي للخصائص المادية والسلوكية للأفراد. يستخدم هذا المصطلح للإشارة إلى البيانات المجمعة عن الأفراد من خلال سماتهم البيولوجية أو الفيزيولوجية كبيانات مسح شبكية العين وقزحية العين وبصمات الأصابع والوجه وتمييز الصوت وهندسة اليد والحمض النووي[15] DNA.

تكمن أهمية استخدام هذه التقنية في إمكانية التحقق من هوية كل فرد تلقائيًا عبر المصادقة البيومترية لسماته المادية والسلوكية، خاصة أن كل فرد يتمتع بسمات فيزيولوجية وتشريحية حية لا يمكن أن تتشابه مع أي فرد آخر، وتعتبر العين إحدى أهم الخصائص الفيزيولوجية إذ أن تغييرها عند الأفراد عملية شبه مستحيلة.

تعمل جميع أنظمة المقاييس الحيوية بالأسلوب نفسه، حيث تُعالج من خلال البرمجة والتشفير السمات الفريدة لكل شخص وتخزنها في قاعدة البيانات. وهناك نوعان رئيسيان من المعرفات البيومترية:
- الخصائص الفيزيولوجية: شكل أو تكوين الجسم (بصمات الأصابع، الحمض النووي، الوجه، اليد، الشبكية، القزحية،...).
- الخصائص السلوكية: سلوك الشخص (الإيقاع، المشية، الإيماءات والصوت...)[16].

• تقنية المصادقة البيومترية

بعد جمع البيانات البيومترية وحفظها في قاعدة بيانات، يُطلب من الفرد التحقق من هويته، فعند تقديمه لبياناته البيومترية للآلة يتم تسجيل البيانات ومقارنتها مع السجل المخزّن في قاعدة البيانات، واذا كانت البيانات مطابقة يتم تأكيد هوية الشخص[17]. يمكن استخدام بعض المعرفات البيومترية، مثل مراقبة ضربات المفاتيح أو المشي في الوقت الحقيقي، لتوفير مصادقة مستمرة بدلاً من التحقق من مصادقة واحدة لمرة واحدة. في حين تستخدم أساليب مصادقة القزحية ونمط الشبكية في بعض أجهزة الصراف الآلي للمصرف، فيما تستخدم الشركات تقنية هندسة اليد أو بصمات اليد وذلك لتسجيل وقت وتاريخ دخول الموظف وخروجه من الشركة. يستخدم عدد كبير من الأجهزة الأمنية حول العالم تقنية التعرف على الوجوه وخاصة في حال أرادت التعرف إلى هويات الأشخاص خلال التجمعات الكبيرة.[18]

• تشفير البيانات البيومترية

تعريف التشفير

التشفير هو تحويل البيانات الإلكترونية إلى شكل آخر، يسمى النص المشفر، والتي لا يمكن فهمها بسهولة إلا من قبل الجهة التي قامت بعملية التشفير أو المرخص لها الوصول إلى هذه البيانات.
يكمن الغرض الأساسي من التشفير في حماية سرية البيانات الرقمية المخزنة على أنظمة الكمبيوتر أو نقلها عبر الإنترنت أو شبكات الكمبيوتر الأخرى. تلعب خوارزميات التشفير الحديثة دورًا حيويًا في ضمان أمن أنظمة تكنولوجيا المعلومات والاتصالات.[19]

التقنيات المعتمدة في التشفير

يشرح الخبير في أمن المعلومات إيلي نصر[20] تقنيتي التشفير الأساسيتين المعتمدتين وهما:
1- Symmetric Encryption أو التشفير المتماثل حيث يتمّ تشفير المعلومات وفكّ تشفيرها بواسطة مفتاح واحد، وهي التقنية التي تستخدمها غالبًا الأجهزة الأمنية في معظم الدول.
2- Asymmetric Encryption أو التشفير غير المتماثل وهي تقنية تستخدم مفتاحين للتشفير، الأول عام والآخر خاص، حيث تخزن البيانات لدى تسجيلها باستخدام المفتاح الأول ويتمّ فكّ التشفير بواسطة المفتاح الثاني، ولا يستطيع سوى من يملك المفتاح الخاص فكّ البيانات المشفرة. تعتمد هذه الطريقة مثلاً المواقع الالكترونية التي يقوم الفرد من خلالها بعمليات البيع والشراء عبر بطاقات الائتمان، أو التي يلج إليها المستخدم من خلال إدخال كلمات سرّ خاصة بحساب في الموقع أو حساب البريد الإلكتروني، وتعتمد هذه التقنية على

اللجوء إلى طرف ثالث يملك البيانات المشفرة لضمان أمن وسلامة البيانات الشخصية.

بدأ الأمن العام اللبناني باعتماد الإقامات البيومترية الذكية منذ هذا العام 2017[21]، علمًا أنه تمّ اتخاذ القرار منذ العام 2014[22]. وبين العام 2014 و2017 أصدر الأمن العام بيانات عدة بشأن هذه الإقامات ووجوب بدء اعتمادها. هذا وبدأ اعتماد جوازات السفر البيومترية في آب/أغسطس 2015[23]، وذلك التزامًا بالمعايير المفروضة من قبل منظمة الطيران المدني الدولي بحسب المديرية العامة للأمن العام[24]. حينها صدر قرارًا عن المديرية العامة للأمن العام بضرورة استبدال جوازات السفر الحالية بأخرى بيومترية خلال فترة وجيزة[25] وقد رافق هذا القرار انتشار اشاعة حول إمكانية رفض بعض الدول دخول حاملي جوازات السفر غير المقروءة آليا إليها[26]، فضلاً عن غياب التوضيح الكافي من قبل الأمن العام حول ماهية جوازات السفر المقروءة آليًا، لا سيما أن البيان الصادر عن الأمن العام في أواخر العام 2015 يشير فقط إلى وجوب استبدال جوازات السفر المجددة بخط اليد أو جوازات سفر تتضمن أسماء مرافقين في حال رغبوا بالسفر.[27]

ولكن، تأخر لبنان في الإيفاء بالتزاماته الدولية. فقد تبلغت الدولة اللبنانية في 31 ديسمبر/كانون الأول 2012 قرار المنظمة الدولية للطيران "ايكاو" بأن الحد الأقصى لصلاحية الجوازات غير المقروءة هي 24 تشرين الثاني/نوفمبر 2015، إلا أنّه تمّ تأخير وقف العمل بالجوازات غير المقروءة آليًا حتى صدر قرار مفاجئ بوجوب ذلك، ما أدى إلى التساؤل إن كان لهذا القرار أي علاقة بجوازات السفر البيومترية.[28]

بحسب رئيس مكتب شؤون الجنسية والجوازات والأجانب في الأمن العام العميد الركن حسن علي أحمد في مقابلة أجرتها معه مجلة الأمن العام اللبناني، اعتبارًا من مطلع عام 2016، أعلنت بعض الدول التزامها بالمعايير المعلنة من قبل المنظمة الدولية للطيران المدني، وبدأت برفض أي جواز سفر غير مقروء آليًا[29]. وينطبق هذا الاجراء على جوازات السفر اللبنانية المجددة التي تحوي مرافقين. وهنا يشير العميد الركن أحمد في المقابلة نفسها إلى طلب الأمن العام السابق بضرورة استبدال هذه الجوازات.

ولكن لمَ فاجأ الأمن العام اللبنانيين ولم يمنحهم الوقت الكافي لتجديد جوازاتهم غير المقروءة آليًا رغم أن منظمة "ايكاو" قد أعلنت في 31 ديسمبر/كانون الأول 2012 أنّ المهلة النهائية لوقف اعتماد الجوازات غير المقروءة آليًا هي 24 نوفمبر/تشرين الثاني 2015؟

يقول الأمن العام اللبناني أنه تزامن قرار الأمن العام وتبليغ البعثات في الخارج بضرورة تجديد جوازات السفر، حيث بدأت الدول تلتزم تباعًا بما طلبته "ايكاو" بحسب تبرير الأمن العام، لذا صدر القرار على عجل في 24 ديسمبر/كانون الأول 2015، وكان الهاجس وفق العميد الركن أحمد ألا يواجه المسافرون أي إشكال في الخارج. ويعتبر الأمن العام الإعلام مسؤولاً عن حدوث هذه البلبلة لعدم دقة مضمون التقارير الإعلامية التي تناولت هذا الموضوع.

اذًا، بدأ اعتماد جوازات السفر البيومترية في شهر آب/أغسطس 2015، بعد أن قررت وزارة الداخلية اللبنانية، بالاتفاق مع المديرية العامة للأمن العام[30]، التوقيع على عقد تلزيم شركة «جيمالتو»، ومقرها أمستردام[31]، لتزويد لبنان عبر شركة «انكريبت» اللبنانية التي يملكها هشام عيتاني[32]، بنظام مراقبة الدخول عبر المرافق الجوية والبرية والبحرية، وإصدار جوازات السفر البيومترية. واللافت أن الشركة الهولندية كانت قد تعرضت لعملية قرصنة لبياناتها المشفرة من قبل وكالة الأمن القومي الأميركي ومركز الاتصالات الحكومية البريطاني.[33]

• تعريف جواز السفر البيومتري

جواز السفر البيومتري هو جواز سفر إلكتروني يحوي شرائح إلكترونية تتضمن معلومات عن صاحب جواز السفر وصورته الرقمية وبصمات أصابع يديه، بحسب الـISO19794[34]. ويمكن للأمن العام في وقت لاحق أن يرفق بهذه الشريحة أي معلومات بيومترية يريدها.

كما أن هذه الشريحة الإلكترونية مرتبطة بنظام معلوماتية مشفّر، والأمن العام هو الجهة الوحيدة التي يمكنها الولوج إلى هذه المعلومات. المعلومات البيومترية المجمعة من المقيمين في لبنان هي نفسها التي يتم جمعها لإصدار الجوازات البيومترية، حيث تتضمن المعلومات الأساسية لحامل الإقامة إضافة إلى صورته الرسمية وبصمات أصابعه.[35]

طرحت SMEX في السابق أسئلة عديدة على الحكومة اللبنانية حول الأنظمة المتوفرة لحماية هذه البيانات وطريقة تخزينها ومن يحق له النفاذ إليها وكيف يتم تشفيرها وحمايتها، والأسئلة نفسها تُطرح اليوم في ما يتعلق بالإقامات البيومترية.

نقلنا الى المديرية العامة للأمن العام، إضافة إلى هذه التساؤلات، أسئلة أخرى حول التنسيق بين الدولة اللبنانية ودول الرعايا الأجنبية وحدود تبادل المعلومات، وكيفية التنسيق مع المفوضية العليا لشؤون اللاجئين. كما طلبنا مقابلة أي من المعنيين المسؤولين عن هذا الملف، إلا أن الأمن العام ردّ بكتاب مقتضب يشير فيه إلى أن جوازات السفر الجديدة تحتوي على عناصر الأمان والثقة بالإضافة إلى انعدام القدرة على تزويرها. وتعتبر البطاقات البيومترية الذكية "تطورًا تقنيًا تنظيميًا يتماشى مع سياسة الأمن العام بتطوير العمل باستمرار". وأفاد كتاب الأمن العام أن التنسيق بين المديرية

والمفوضية العليا لشؤون اللاجئين يتم من خلال آليات خاصة ومذكرة تفاهم موقعة منذ العام 2003، وان الإقامات البيومترية تسجّل جميع الرعايا الأجانب المستحقين ومنهم السوريون الذين استوفوا شروط الإقامة.
لم يقدم الأمن العام جوابًا عن التقنية التي يستخدمها في تشفير البيانات. ولكن، نتيجة معرفته واطلاعه على التقنيات المستخدمة في عدد من دول العالم، يرجّح الخبير في أمن المعلومات ايلي نصر أن يعتمد الأمن العام التقنية الأولى في التشفير، ويمكن أن يلجأ إلى استخدام التقنية الثانية لنقل البيانات عبر شبكة الإنترنت أو عبر شبكة تربط الأجهزة والمراكز ببعضها، إلا أنه يبقي على التقنية الأولى في تشفير البيانات الأساسية.
يمكن تزوير جواز السفر، ويمكن أيضًا تقليد الرقاقة المرفقة به، ولكن يتم كشف التزوير عند مطابقة رمز جواز السفر والرمز المحفوظ في ملفات الأمن العام. فالمعلومات المرفقة بالرقاقة تشكل رمزًا خاصًا بحامل جواز السفر ولا يعرف هذا الرمز سوى الأمن العام. ولكي لا يقوم المزورون بكشف الرمز من خلال استخدام المنهجية نفسها التي اعتمدها الأمن العام في وضع الرمز، على هذا الأخير أن يضيف على البيانات أرقامًا أو رموزًا تجعل من تزوير الجواز مهمة صعبة جدًا، إلا في حال تسرّبت هذه البيانات من داخل الأمن العام.

يؤكد نصر أن جوازات السفر المقروءة آليًا وجوازات السفر البيومترية لا تختلف من ناحية تخزين البيانات أو ناحية تشفيرها إلّا أن البيانات البيومترية تتمتع بخاصية التعرف التلقائي على الأفراد، ويمكن للأمن العام أن يرفق مع البيانات الأساسية التي يجمعها عن الأفراد أي بيانات إضافية يريدها، كما يمكنه أن يحدد المعلومات المسموح لموظفي الأمن الاطلاع عليها على المعابر الحدودية أو داخل مراكزه والمعلومات الأخرى التي يُحظر الاطلاع عليها.

تُحفظ بيانات الإقامات على خادم مختلف عن ذاك الذي تُخزّن فيه بيانات جوازات السفر، إلا أن تقنيات التخزين المُعتمدة هي نفسها، وقد تختلف قليلًا في التشفير. ويمكن للحكومة اللبنانية تبادل هذه المعلومات مع دول أخرى من خلال اتفاقية بين الدولتين، كالاتفاقية العربية لمكافحة الإرهاب التي ذكرنا سابقًا أن لبنان عضو فيها منذ العام 1999، حيث تتعهد كل من الدول المتعاقدة، بتزويد أي دولة متعاقدة أخرى، بما يتوافر لديها من معلومات أو بيانات من شأنها أن تساهم في مكافحة الإرهاب، ومن بين البيانات التي يمكن تبادلها "أوصاف الشخص المطلوب تسليمه بأكبر قدر ممكن من الدقة، وأي بيانات أخرى من شأنها تحديد شخصه وجنسيته وهويته". وعلى كل دولة من الدول المتعاقدة أن تقوم بحسب المادة الثالثة من الاتفاقية بإنشاء قاعدة بيانات لجمع وتحليل المعلومات الخاصة بالعناصر والجماعات والحركات والتنظيمات الإرهابية ومتابعة مستجدات ظاهرة الإرهاب والتجارب الناجحة في مواجهتها وتحديث هذه المعلومات وتزويد الأجهزة المختصة في الدول المتعاقدة بها، وذلك في حدود ما تسمح به القوانين والإجراءات الداخلية لكل دولة.

• اعتماد التقنية البيومترية الذكية في جوازات السفر والإقامات

يتم تبادل المعلومات عبر استخدام الدولة اللبنانية لبرنامج معلوماتي (يختلف عن ذاك المستخدم لتخزين بيانات الإقامات) حيث تعطي من خلاله الدولة الأخرى الحق بالولوج إلى معلومات محددة تقوم السلطات بوضعها على خادم الجهاز، ويجري تحديثها بشكل دوري. تقنيًا، العملية بسيطة، إذ يكفي أن يتمتع هذا البرنامج بخاصية قراءة الباركود أو الرقاقة.

وبالتالي، في غياب قانون ينظم عملية تشفير وتخزين البيانات البيومترية، وضعف الحماية القانونية للبيانات الشخصية في لبنان، لا يمكن اعتبار عملية تشفير المعلومات سوى تدبير لحماية هذه المعلومات من القرصنة، ولا يمكن أن يعتبر التشفير ضمانة لحماية البيانات الخاصة، ما لم يكن هناك قانون وإجراءات تحمي هذه البيانات من أي انتهاك للحق في الخصوصية والحق في حماية البيانات الشخصية من قبل الأجهزة الرسمية نفسها.

القسم الثالث: قضايا حديثة عن خروقات البيانات الشخصية وإساءة استخدامها

• بيانات المرضى: نموذج مستشفى الجامعة الأمريكية

في شهر أبريل/نيسان من العام 2012 طلبت إدارة الجامعة الأميركية في بيروت من قسم المعلوماتية في الجامعة الحصول على كافة البيانات المخزنة على أجهزة الكمبيوتر داخل الحرم الجامعي والمركز الطبي. اعترض حينها قسم المعلوماتية لكون البيانات تشمل كل المراسلات الإلكترونية بين أهل الجامعة من أساتذة وطلاب وموظفين والتي تتم عبر البريد الالكتروني الخاص بالمؤسسة، أي الذي ينتهي بـ «aub.edu.lb». كذلك يتضمن طلب الإدارة وضع يدها على المعلومات الشخصية والمهنية للموظفين والمعلومات الحساسة الخاصة بالأطباء وفريق العمل والمرضى في مستشفى الجامعة.[36]

وأرادت الإدارة اتخاذ هذه الخطوة بسبب تسريب معلومات حساسة عن الجامعة والسياسة التي يتبعها الإداريون فيها، الأمر الذي اعتبرته الجامعة مسيئًا بحقها، لذا طلبت البيانات لمعرفة من يسرّب معلومات عن الجامعة والخفايا التي تدور على بريدها الإلكتروني.[37]

حينها طُرحت تساؤلات عدة حول مصير هذه البيانات وإلى أي مدى هي محمية، خاصة أن الجامعة نفسها قد لفتت إلى أن "البيئة التقنية للجامعة الأميركية في بيروت غير آمنة"[38]، ونُقلت قاعدة بيانات الجامعة من قسم إلى أخر، بما فيها بيانات المركز الطبي التابع للجامعة الأميركية في بيروت. وتكررت بعدها عمليات تسريب المعلومات[39]، حيث كان لحسين مهدي، وهو أحد مُعدي التقرير دور في إبرازها من خلال نشره لعدد من هذه البيانات في إحدى الصحف اللبنانية[40]، وذلك في سبيل كشف حالات الهدر والفساد وسوء الإدارة وغيرها من الأمور في الجامعة الأميركية ومركزها الطبي[41]. تطرح هذه التسريبات المتكررة تساؤلات جدية حول الأنظمة المعتمدة لحماية بيانات المرضى الذين يلجأون إلى المركز الطبي التابع للجامعة، والأنظمة المعتمدة في مستشفيات أخرى.

لم يجب كلٌّ من المركز الطبي في الجامعة الأميركية، ومستشفى بيروت الحكومي، ومستشفى أوتيل ديو على رسائلنا، في حين اعتبر قسم المعلوماتية في مستشفى جبل لبنان أن هذه المعلومات سرية ولا يمكن الإفصاح عن اسم البرنامج الذي تستخدمه المستشفى واذا ما كان آمنًا أو لا.

ينبع طرح هذه التساؤلات من مخاوف عديدة حول إمكانية خرق هذه الأنظمة، فأحدث التقارير التي طالت الجامعة الأميركية في بيروت حول موضوع تسريب البيانات، كان تقرير غير منشور صادر عن لجنة شركة FTI consulting يفيد بأن نظام المعلوماتية في الجامعة "هش" ولم تستطع الشركة معرفة مصدر التسريب. والأهم، حصول أحد مُعدي هذا التقرير على ملفات طبية من داخل المركز الطبي في الجامعة الأميركية بعدما علم بعملية اختراق لنظام المركز، ما يؤكد أن هذه البيانات التي يُفترض أن تكون محمية بموجب القوانين المرعية الإجراء، لا تخضع لأي شكل من أشكال الحماية وخصوصية المرضى بالتالي معرضة للخطر. أكثر المستفيدين من هذا التسريب بحسب مصدر من داخل الجامعة هم شركات التأمين التي تسعى بطرق عدة لمعرفة كافة التفاصيل الخاصة بحالة زبائنها الصحية. وتعليقًا على الموضوع، يقول رئيس الهيئة الوطنية الصحية الطبيب إسماعيل سكرية أن وصول هذه البيانات إلى شركات التأمين يؤثر على علاقة المواطن بالشركة التي يتعامل معها، فيمكن حينها للشركة أن تمتنع عن تجديد بوليصة التأمين أو أن ترفع التعرفة في حال وجدت من خلال الملف الطبي أن الزبون مُعرّض أو قد يتعرض للإصابة بأمراض مزمنة أو أمراض تتطلب علاجًا مكلفًا.

• أرقام الهواتف الخلوية الشخصية

يصل بشكلٍ يوميٍّ إلى أرقام الهواتف الخلويّة وعناوين البريد الإلكتروني الخاصة باللبنانيّين والمقيمين في لبنان، رسائل نصّية قصيرة ورسائل بريديّة من قبل عشرات الشّركات التّجاريّة والجمعيّات والمؤسّسات والبلديّات والأفراد وغيرهم، وذلك من دون الحصول على إذن مسبق من هؤلاء المواطنين، ما يشكّل انتهاكًا للحق في الخصوصية والحق في حماية البيانات الشخصيّة.

لا تقدّم شركات الخلوي في لبنان خدمة منع وصول رسائل نصّية تجارية إلى المواطنين، ولكنّها تسمح لهم فقط في أن يمنعوا تكرار وصول الرسالة من المصدر نفسه. يتطلب تفعيل هذه الخدمة اتصال المواطن بمندوبي الشركة وتزويدهم باسم المرسل، بحسب ما أكّد مندوبو الشركتين لدى اتّصالنا بالرقم المخصص للزبائن 111. يبلغ متوسط تكلفة ارسال 1000 رسالة نصية 45 دولارًا أمريكيًا تقريبًا ويصل إلى 11 ألف دولار أمريكي لإرسال 500 ألف رسالة نصية. كذلك يصل متوسط تكلفة إرسال 50 ألف بريد إلكتروني إلى 150 دولارًا أمريكيًا، بينما يصل متوسط تكلفة إرسال 360 ألف بريد إلكتروني إلى 430 دولارًا أمريكيًا، وذلك وفق العروض التي حصلنا عليها من الشركات التي تواصلنا معها خلال إعداد التقرير.

الرسائل النصية القصيرة	السعر (بالدولار الأمريكي)	رسائل البريد الإلكتروني	السعر (بالدولار الأمريكي)
1,000 رسالة	45	50,000 رسالة	150
5,000 رسالة	150	100,000 رسالة	270
10,000 رسالة	300	160,000 رسالة	290
50,000 رسالة	1,300	360,000 رسالة	430
100,000 رسالة	2,500		
500,000 رسالة	11,000		

إذاً، البيانات الخاصّة باللبنانيّين عرضة لعمليّات البيع والشراء المستمرة، سواء من خلال شركتي تاتش وألفا، أو من خلال شركات الإعلانات التي تقدّم خدمات إرسال الرسائل النصية القصيرة sms ورسائل البريد الإلكتروني وذلك تبعًا للفئة التي يُحدّدها العميل أو من خلال شركات الإعلانات المُتخصّصة في إرسال هذا النوع من الرسائل. تعترف شركتا تاتش وألفا باستخدام بيانات المشتركين المسجّلة لديها لبيعها إلى شركات تجارية أو أفراد يوّدون إرسال رسائل نصّية قصيرة إلى فئة مستهدفة، وهي محدّدة وفق ما يشير كل من الموقع الإلكتروني لألفا[42] وتاتش[43] حول جنس الفئة المستهدفة وعمرها وطبيعة عملها وهي البيانات التي تحصل عليها الشركتان لحظة شراء المواطنين للخطوط المدفوعة سلفًا أو عند تثبيت خطهم، أو لاحقًا عند اتّصال موظفي الشركة بهم.

إلا أنَّ هناك معيارًا إضافيًا مثيرًا للشكوك تقدمه شركة تاتش بحيث يُمكن للعميل أنْ يرسل الرسائل استنادًا إليه، وهو "سلوك استخدام الشبكة" Usage Behavior وبيانات خاصّة أخرى. فكيف تقوم الشركة بتخزين هذه البيانات، ولماذا تقوم الشركة نفسها بتخزين بيانات عن "سلوك استخدام الشبكة" بهدف بيعها؟ وما هي الإجراءات التي تتبّعها الشركتان في حماية هذه البيانات من التسريب، وهل تقوم الشركات التجارية التي تقدّم خدمة الرسائل النصّية القصيرة بشراء هذه البيانات من شركتي الخلوي؟ خاصّةً أن معظم هذه الشركات تدعي بأنها تستخدم مسلك route الشبكتين في إرسال الرسائل. وقد نقلنا تساؤلاتنا إلى شركتي الخلوي للحصول على بعض التفاصيل، إلا أننا لم نتلقَ أي ردود.

في مقابلة مع SMEX قال المحامي طوني مخايل إن القانون 431/2002 الذي يُعنى بتنظيم قطاع خدمات الاتصالات لم يلحظ في أي من مواده مسألة حماية البيانات الشخصية. ويلفت مخايل الى أن قانون الحق في الوصول إلى المعلومات، الذي أقر مؤخرًا داخل المجلس النيابي يحمي بيانات اللبنانيين، إلّا أن هذه الحماية تقتصر فقط على منع المؤسّسات العامّة من تزويد أيٍّ كان بمعلوماتٍ خاصة وشخصية عن المواطنين، وهو في حال تطبيقه قد لا يحلّ سوى جزء بسيط من قضية انتهاك الحق في حماية المعلومات الشخصية.

على المستوى التقني، وفي ما يتعلق بشركات الاعلانات التي تقدّم الخدمة نفسها، اتّصلنا بشركاتٍ اخترناها بشكل عشوائي، لنحصل على معلومات وافية منها حيث طلبنا تزويدنا بعرض أسعار للخدمات المُقدّمة والاستفسار عن بعض المعلومات الإضافية. أفادت جميع الشركات التي اتصلنا بها بأنه بإمكان العميل أن يختار الفئة العمرية والجنس ومكان السّكن أو محل القيد وطبيعة العمل وغيرها من البيانات الخاصة بالأفراد، رافضةً الإفصاح عمّا إذا كانت تحصل على هذه البيانات من شركتي تاتش أو ألفا.

سمحت شركة Bestsmsbulk لنا باستخدام حساب تجريبي، للاطلّاع على طبيعة البيانات الخاصة المُجمّعة لديها عن المواطنين، وعندما سألنا عن مدى دقّة هذه البيانات وإمكانية التلاعب بها عبر إرسال رسائل إلى أرقام عشوائيّة، بدلاً عن الفئة المحددة من قبل العميل، أفادت الشركة بأنه بعد إرسال الرسائل النصية القصيرة sms إلى الفئة المستهدفة، تقوم الأخيرة بتزويد العميل بتقرير يحوي الأرقام التي وجّهت إليها الرسائل، ولكنها أرقام غير مكتملة أي مشفرة، عندما يختار عددًا من هذه الأرقام، فتُظهر الشركة الرقم كاملاً في حال أراد العميل الاتصال به للتأكّد من توافق بياناته الشخصية مع المعايير التي جرى اختيارها.

أما شركة Best 2 sms فقدّمت لنا عرضًا سريعًا عبر الهاتف موضّحة أن هذه البيانات يجري تحديثها بشكل دوري ويتم الحصول عليها من مصادر عدّة منها بيانات تحصل عليها من بعض البلديات، وبيانات رخص السّير والسوق التي تتسرّب بشكل سنويّ، وتطبيقات الهواتف الذكية، وجدول عامّ نقابة المحامين، ومصادر أخرى. ونلاحظ أن المعلومات الشخصية الخاصة بالمواطنين اللبنانيين تدخل في مزاد بيع وشراء من قبل شركات الإعلانات وشركات الخلوي من دون حسيب أو رقيب.

• أرقام لوحات تسجيل السيارات

يجري تسريب كافة بيانات السيارات المسجلة لدى مصلحة تسجيل السيارات (النافعة) على أقراص مدمجة يحصل عليها السماسرة أولًا ثم تُسرّب وتباع الى المواطنين. تحتوي هذه الأقراص المدمجة على بيانات خاصة وشخصية مثل الاسم الثلاثي لصاحب السيارة المسجلة مع تاريخ ومكان ولادته ورقم سجله ومكان إقامته بشكل مفصّل ورقم هاتفه الخاص ورقم هاتف المنزل.[44]

إن الوصول إلى هذه الأقراص المدمجة سهل جدًا، فقد أنجزت في وقت سابق الوحدة الاستقصائية في قناة الجديد[45] تحقيقًا بعنوان "رالي الجمارك: سباق التهرب الضريبي" تناولت فيه قضية تهرب عدد من كبار السياسيين ورجال الأعمال وفنانين وغيرهم من دفع الرسوم الجمركية لسياراتهم، وقد استطاع فريق العمل أن يحصل على لائحة المواطنين اللبنانيين والمقيمين الذين قاموا بعملية "ادخال مؤقت" لسياراتهم (وهي الطريقة التي من خلالها تتم عملية التهرب من دفع الرسوم)، وذلك من خلال الحصول على أقراص مدمجة فيها ما يكفي من بيانات شخصية عن كافة المواطنين والمقيمين الذين يمتلكون سيارات في لبنان، وهي بيانات غير مشفرّة وغير محميّة، وقد تم تحفيظها من خلال برنامج Microsoft Excel وبرنامج بدائي آخر.[46]

طوال السنوات الماضية لم تقم السلطات المعنية بأي إجراء لمكافحة هذه الظاهرة، علمًا أنها لا تشكل فقط انتهاكًا لخصوصية المواطنين، بل تعرضهم لخطر حقيقي، حيث أشارت تقارير صحفية عدة إلى أنه قد تقع هذه الأقراص المدمجة بيد عصابات تمتهن سرقة السيارات وسلبها، بحيث يعمد أفراد هذه العصابات إلى استخدام اللوحات الأصلية لهذه السيارات على سيارات مسروقة من نفس النوع والطراز واللون تكون بحوزتهم، ومن ثم يزوّرون أوراقها بغية بيعها[47]. لا يمثّل هذا الأمر فقط خطرًا على أمن المواطن، بل إنه أيضًا خرق خطير لأمن المجتمع وسلامته، إذ إن أرقام اللوحات المسرّبة بهذه الطريقة قد تستعمل في أعمال إرهابية أو في تنقّل مطلوبين للعدالة وفق تصريح أدلى به رئيس مكتب مكافحة السرقات الدولية في وحدة الشرطة القضائية، العقيد فؤاد خوري.[48]

بالعودة إلى موضوع الخصوصية، هناك تطبيقات تظهر من وقت لآخر وتُحذف بعد فترة إثر شكاوى المواطنين الذين تُنتهك خصوصيتهم، كتطبيقcars961 مثلًا الذي تم حذفه بعد فترة وجيزة، حيث يمكن بواسطته الحصول على التفاصيل الشخصية الخاصة بأي مواطن من خلال رقم سيارته المسجلة.[49]

إنّ اعتماد الدولة اللبنانية دفاتر سوق بيومترية منذ 4 يناير/كانون الثاني 2017 عبر تلزيم شركة Inkript، وهي الشركة نفسها التي كُلفت بمسألة إصدار جوازات السفر البيومترية، لا يعني بأن هذه البيانات ستبقى محمية، طالما أن هيئة إدارة السير لم تقرر بعد اعتماد أنظمة حماية المعلومات التي تُحفظ على أجهزة مصالح تسجيل السيارات، وفق ما أفاد به الخبير في أمن المعلومات إيلي نصر.

القسم الرابع: مشروع قانون المعاملات الإلكترونية وحماية البيانات الشخصية

تعود الخطوة الأولى المتخذة لوضع تشريع خاص بحماية البيانات الشخصية إلى عام 2005، عندما جرت صياغة أول مسودة لمشروع قانون يتعلق بالاتصالات والكتابة والمعاملات الإلكترونية. وقد أعدت هذه المسودة في مرحلة سابقة، وأطلقت في إطار EcomLeb بمبادرة من وزارة الاقتصاد والتجارة وبدعم مادي من الاتحاد الأوروبي. لاحقًا، في آب 2010، قدمت اللجنة الاستشارية في البرلمان اللبناني برئاسة النائب غنوة جلول نسخة معدلة عن مشروع قانون EcomLeb أثارت ردود فعل سلبية من قبل منظمات المجتمع المدني والوسط القانوني.[50] ومع بداية كانون أول/ديسمبر 2011 تقدم النائب بطرس حرب باقتراح قانون يتعلق بالمعاملات الإلكترونية، مستندًا إلى الدراسة ذاتها.[51]

حاليًا، تجري مناقشة "مشروع قانون المعاملات الإلكترونية والبيانات الشخصية" أمام لجنة فرعية منبثقة عن اللجان النيابية الدائمة. ويشارك في النقاشات ممثلون عن الوزارات المعنية مثل وزارة الاقتصاد، والداخلية، والاتصالات، بالإضافة إلى ممثل عن مكتب مكافحة جرائم المعلوماتية، ومصرف لبنان، ونقابة المحامين وقضاة وأكاديميين. في إطار مقابلة أجرتها منظمة SMEX مع عدد من محامي مركز المعلوماتية وتكنولوجيا الاتصالات في نقابة المحامين في بيروت، اعتبر المركز أنّ مشروع القانون "هجين كونه نتيجة لصياغات مقدمة من عدة وزارات وجهات، إلا أن النقاشات ستؤدي إلى تخفيف التناقضات". إلى ذلك، يوجه المركز مشاركته خلال النقاشات باتجاه ضمان إقرار هذا القانون نظرًا للحاجة الماسة إليه:

> "يقوم الناس اليوم بمعالجة أي بيانات وكافة البيانات، ما يعني أن وضع إطار تشريعي سيؤدي إلى تنظيم هذه المسألة ووضع ضوابط وعقوبات. بهذه الطريقة تتم حماية الحقوق والحريات."

في البداية، سجل أعضاء مركز المعلوماتية مجموعة من الملاحظات حول النقاش الذي يدور في اللجنة الفرعية. ومن بينها مثلاً استغرب المركز أن تكون وزارة الاقتصاد هي الجهة المسؤولة عن تلقي تصاريح معالجة البيانات فيما يبدو أقرب إلى المنطق أن تكون وزارة الاتصالات هي صاحبة الصلاحية في هذا المجال، لا سيما أن أمن البيانات الشخصية يرتبط بجزئه الأوسع حاليًا بتكنولوجيا الإنترنت والاتصالات.

> "كان مستشارو الوزارات يحضرون الاجتماعات بشكل أساسي لتمرير المسائل المرتبطة بوزاراتهم كما هي وحفظ صلاحيات لها في القانون، فحصل مثلاً "شد حبال" بين وزارتي الاقتصاد والاتصالات. كما رفض مصرف لبنان أي نقاش في الجزء المتعلق بالمعاملات المصرفية فتمّ إدراج هذا الباب في القانون كما قدمه مصرف لبنان من دون نقاش."

من جهته يؤكد مركز المعلوماتية أن لنقابة المحامين أولوياتها بالنسبة لهذا القانون، وهي حماية الحقوق وصونها، ويحاول المركز الاستفادة من مشاركته في المناقشات للوصول إلى هذا الهدف:

> "كل مسألة تثير الشكّ من حيث آثارها ومضمونها تدفعنا إلى خوض معركة لتعديلها. فعلى سبيل المثال، دار نقاش حاد حول الصلاحيات الواسعة التي تتمتع بها النيابة العامة التمييزية في ما يتعلق بحظر المواقع الإلكترونية. ففي الواقع، يجمع النائب العام اليوم من خلال منصبه بين 3 سلطات، ألا وهي الملاحقة والتحقيق واتخاذ القرار، وهو ما يخالف معايير العدالة والحق في الانتصاف. يقوم حاليًا مكتب مكافحة الجرائم المعلوماتية بإحالة لائحة بالمواقع التي يراها مخالفة للآداب العامة أو للقوانين الى النائب العام، فيصدر هذا الأخير قرارًا بحجبها ويحفظ الملف، بالتالي لا يعود من الممكن حتى المراجعة فيه أو الاعتراض عليه."

لا يجد مركز المعلوماتية أن هناك أي حاجة لوجود جهة قضائية متخصصة بموضوع حماية البيانات الشخصية. أما من ناحية الملاحقة والتحقيق في الجرائم المرتبطة بهذا المجال فيجد أنه من الأفضل إنشاء نيابة عامة متخصصة. كما يوضح مركز المعلوماتية أن جهوده تنكب بشكل أساسي على العمل على الباب الخامس المتعلق بحماية البيانات الشخصية. وفي هذا الإطار يشير إلى مجموعة من المواد يرى أن هناك ضرورة لتعديلها. لذا سنستعرض في ما يلي مضمون الفصول الخمسة المكونة للباب الخامس، حيث ستشمل أيضًا النقاط التي لا تزال رهن النقاش.

• مضمون الباب المتعلق بحماية البيانات الشخصية (الباب الخامس)

الفصل الأول – الأحكام العامة المتعلقة بحماية البيانات الشخصية

لم تسجل نقابة المحامين أي اعتراض على ما يتضمنه مشروع القانون في هذا الفصل. وتخضع لأحكامه كل المعالجات الآلية أو غير الآلية للبيانات الشخصية، باستثناء المعالجات المتعلقة بالنشاطات الحصرية التي يقوم بها الشخص حصرًا لحاجاته. يكرس هذا الفصل المبادئ والحقوق التالية:

• **قانون يتعلق بالنظام العام:** ينص الفصل الأول من الباب الخامس على عدم جواز الاتفاق على مخالفة الأحكام الواردة في هذا الباب.

بالتالي تنازل صاحب البيانات ذات الطابع الشخصي عن حقوق مكرسة له بموجب هذا القانون يبقى بلا قيمة قانونية. بهذا المعنى، يكرس مشروع القانون الأحكام الواردة ضمنه على أنها من النظام العام، وهذا يعني أن أي مخالفة لأحكامه تخضع للملاحقة والابطال بغض النظر عن إرادة الشخص المنتهكة حقوقه القيام بهذه الملاحقة.

• **الحق في الاطلاع:** يُعد الحق في الاطلاع من الضمانات الأساسية لعدم تعسف أي شخص عام (إدارة عامة، بلدية، موظف عام...) أو خاص (شركة خاصة، مؤسسة، أي شخص عادي) في استعمال سلطته عند معالجته البيانات الشخصية للأفراد. وفقًا للمادة 86 من مشروع القانون، فإن "لكل شخص الحق في الاطلاع والاعتراض أمام المسؤول عن معالجة البيانات الشخصية، على المعلومات، والتحاليل المستعملة في المعالجة الآلية المتعلقة به والمُتذرع بها بوجهه."

الفصل الثاني – جمع المعلومات الشخصية ومعالجتها

لا يشمل هذا الفصل أيضًا أي مواد تثير اعتراض نقابة المحامين. وينصّ مشروع القانون على عدد من الشروط الضرورية لحماية البيانات الشخصية، أثناء معالجتها، وتشمل تحمّل "المسؤول عن المعالجة" مسؤولية مركزية في هذا المجال. فتنص المادة الأخيرة من الفصل (المادة 93) على وجوب "أن يتخذ جميع التدابير، بحسب طبيعة البيانات والمخاطر الناتجة عن المعالجة، لضمان سلامة البيانات وأمنها ولمنع تعرضها لتشويه أو تضررها أو وصولها إلى أشخاص غير مخولين الاطلاع عليها."

أما الشروط التي يفرضها هذا الباب فهي التالية:
المعالجة الآمنة والمشروعة
"تُجمّع البيانات ذات الطابع الشخصي بأمانة ولأهداف مشروعة ومحددة وصريحة." (المادة 87)

• الالتزام بالغاية المحددة للجمع، على أن تكون الغاية مشروعة وواضحة: "يجب أن تكون البيانات ملائمة وغير متجاوزة للأهداف المعلنة، وأن تكون صحيحة وكاملة وأن تبقى ميومة بالقدر اللازم." (المادة 87)

• الالتزام بالفترة المحددة للمعالجة: "لا يمكن في مرحلة لاحقة معالجة هذه البيانات لأهداف لا تتوافق مع الغايات المعلنة، ما لم يتعلق الأمر بمعالجة بيانات لأهداف إحصائية أو تاريخية أو للبحث العلمي." (المادة 87)

"لا يكون حفظ البيانات ذات الطابع الشخصي مشروعًا إلا خلال الفترة المبينة في التصريح عن المعالجة أو في القرار الذي يرخِّص بها." (المادة 90)

• تحصين البيانات المتعلقة بالحالة الصحية أو الهوية الوراثية أو الحياة الجنسية للأشخاص: "يُمنع جمع البيانات ذات الطابع الشخصي أو معالجتها، إذا كانت تكشف، بصورة مباشرة أو غير مباشرة، عن الحالة الصحية أو الهوية الوراثية أو الحياة الجنسية للشخص المعني."

على أن المادة نفسها تذكر استثناءات على هذا المنع في أربع حالات:

• عندما يكون الشخص المعني قد وضع هذه البيانات في متناول الجمهور أو وافق صراحةً على معالجتها، ما لم يكن هناك أيّ مانع قانوني.

• عندما يكون جمع البيانات أو معالجتها ضروريًا لوضع تشخيص طبي أو تقديم علاج طبي من قبل عضو في مهنة صحية (يذكر في هذا المجال أن القوانين الراعية لهذه المهنة تفرض السرية وتعاقب على خرقها)

• عند إثبات حق أو الدفاع عنه أمام القضاء.

• في حال الحصول على ترخيص وفق أحكام المادة 97 من هذا القانون. ويكون وزير الصحة العامة الجهة المختصة بمنح هذا الترخيص وفقًا للمادة المذكورة.

الفصل الثالث – الإجراءات المطلوبة لوضع المعالجات قيد التنفيذ

• **التصريح والترخيص**
إنّ الإختلاف بين التصريح والترخيص جوهري. فالأول لا يلزم الشخص سوى بإعلام الجهة المختصة بالعمليات التي يريد أن يقوم بها وفقًا

للقانون وفي إطار أحكامه. بالتالي هو مجرد إعلام وليس رهن قبول الإدارة أو رفضها. وخلافًا لذلك، بإمكان الإدارة أن تمنح ترخيصًا لطالبه أو أن ترفضه، وذلك بعد التأكد من الشروط الواجب توافرها لحيازته هذا الترخيص.
تحدد المادة الأولى من هذا الفصل (المادة 94) الجهات المخولة معالجة البيانات من دون أي تصريح مسبق. وتجد نقابة المحامين أنه يجب إعفاء نوعين إضافيين من المعالجات من وجوب الحصول على تصريح: المعالجات التي يقوم بها أشخاص الحق العام كلّ في إطار صلاحياته، والمعاملات التي نصّ عليها قانون التنصت الذي ينظم آليات اعتراض المكالمات الهاتفية.

في ما يختصّ بالقانون 140/1999 أو ما يعرف بقانون التنصت، فإنه ينظم آليات الحصول على ترخيص لاعتراض الاتصالات ومراقبتها. ووزارة الاتصالات هي الجهة المختصة بمنح هذا الترخيص. بالتالي فإن هذه الإضافة ضرورية لحماية البيانات المعالجة إثر اعتراض مكالمة من جهة، ولمنع حصول تضارب في الصلاحيات من جهة ثانية بين وزارة الإتصالات المتخصصة بموجب قانون التنصت بمنح تراخيص اعتراض المكالمات، ووزارة الاقتصاد صاحبة الاختصاص العام بمنح التراخيص بموجب مشروع القانون المتعلق بالمعاملات الالكترونية وحماية البيانات الشخصية. لا سيما أن تضاربًا مماثلًا في الصلاحيات قد يشكل بابًا واسعًا لانتهاك بيانات الأفراد تحت غطاء قانوني.

أما في ما يتعلق بأشخاص الحق العام، والمقصود بهم كل الإدارات والمؤسسات التابعة للدولة اللبنانية، المركزية منها والمحلية (الوزارة أو البلدية)، فتبدو مسألة إعفائهم من الحصول على تصريح بديهية، كونه من غير المنطقي أن يُطلب إلى الدولة أنتمنح نفسها تصريحًا عبر إحدى وزاراتها لمعالجة بيانات مواطنيها أو المقيمين على أرضها. وبعكس ذلك، تكون الأولوية لتضمين القانون نفسه أكبر قدر من الضمانات لحقوق الأفراد، لا سيما حقهم في الاعتراض والانتصاف أمام المحاكم في حال انتهاك حقهم في احترام خصوصية بياناتهم، وتأمين كل الضمانات اللازمة لمنع تعسف أشخاص الحق العام باستخدام امتيازاتهم بمواجهة الأفراد.

بالتالي فإن التصريح هو الأصل بالنسبة لمشروع القانون، أي أن المعالجة بشكل عام تتم وفقًا لتصريح، غير أن بعض البيانات بحاجة لترخيص من أجل معالجتها. وهي ثلاث فئات:
1- البيانات المتعلقة بالأمن الخارجي والداخلي للدولة بموجب قرار مشترك يصدر عن وزيري الدفاع الوطني والداخلية والبلديات
2- البيانات المتعلقة بالجرائم الجزائية وبالدعاوى القضائية بموجب قرار يصدر عن وزير العدل
3- البيانات المتعلقة بالحالات الصحية أو بالهوية الوراثية أو بالحياة الجنسية للأشخاص بموجب قرار يصدر عن وزير الصحة العامة.

• مهلة إصدار الترخيص

لا تنص المادة بصيغتها الحالية على مهلة محددة لمنح الترخيص أو رفضه. أما نقابة المحامين فتعتبر أنه لا بد من ربط قرار الجهات المذكورة بمهلة واضحة بحيث لا تتحول هذه المادة إلى باب لمنع معالجة هذه البيانات بالطرق القانونية وضمن الضمانات التي ينص عليها القانون. وسيؤدي ذلك إلى العودة إلى المعالجة غير المنظمة للبيانات الشخصية. بالتالي تقترح نقابة المحامين إضافة فقرة تحدد مهلة واضحة لصدور قرار الترخيص (شهران من تقديم الطلب)، على أن يُفسر صمت الجهة المختصة بمنح الترخيص على أنه "قبول ضمني" بعد انقضاء هذه المهلة.

• الجهة المختصة بتلقي التصاريح

يحدد هذا الفصل الوزارة التي تستقبل طلب تصاريح معالجة البيانات، وهي وزارة الاقتصاد والتجارة، ويُفصل البيانات التي يجب أن يتضمنها التصريح (المادة 96)، ومن واجب وزارة الاقتصاد والتجارة تجاه "الجمهور" نشر مجموعة من المعلومات المتعلقة بجامع البيانات (المادة 98).

الفصل الرابع – حق الوصول والتصحيح

يبدو لافتًا تخصيص فصل كامل لهذا الحق، وهو ما يعكس منحه أهمية فائقة بالمبدأ. فيعتبر حق الوصول، أي وصول صاحب البيانات إلى البيانات المجموعة عنه والتي تخضع للمعالجة، وهو ما يعرف أيضًا بالحق في الاطلاع، ضمانة أساسية لحماية بيانات الأشخاص من أي انتهاك أو تمادٍ في جمعها ومعالجتها، أو استخدامها لغير الغاية التي جُمعت لها. كذلك الأمر بالنسبة لحق التصحيح، فإنه يحمي الأشخاص من تناقل بيانات خطأ عنهم أو نشرها، أو معالجتها بأي طريقة من طرق المعالجة.

أهمية هذا الفصل جعلته موضع نقاش واختلاف في وجهات النظر أكثر من غيره، حيث تقترح نقابة المحامين تعديلات على مجمل مواده. إذاً يتضمن هذا الفصل حق صاحب البيانات بالحصول عليها، بالإضافة إلى طلب تصحيحها أو تحديثها أو محوها، والحق باللجوء الى "المرجع القضائي المختص لا سيما قاضي الأمور المستعجلة". بالمقابل يتضمن حقوق مُعالج البيانات، كأن يطلب بدلاً (مالياً) عن تنفيذ طلب المعالجة، أو أن يرفض الطلبات التي تتسم بطابع التعسف.

واقتصر انتقاد نقابة المحامين على توصيف الشخص الذي يتمتع بهذا الحق. ففيما يمنح النص الحالي للمشروع "كل صاحب صفة" الحق في

الوصول والتصحيح، تتمسك النقابة بضرورة استبدال هذه العبارة أينما وردت في هذا الفصل بـ"صاحب البيانات أو أي من ورثته"، وهو تعبير أكثر حصرية يضمن للأفراد حقهم في الخصوصية.
كما تقترح نقابة المحامين حذف عبارة: "يحق لورثة الشخص الطبيعي ذي الصفة مطالبة المسؤول عن المعالجة بإدخال التعديلات المستجدة بعد وفاة مورثهم". ويعود ذلك إلى استحالة اعتراض الميت على المعلومات الخطأ التي قد ترد عنه في حال السماح بتعديل بياناته بعد الوفاة، ما يؤدي بالضرورة إلى تعليق أي عملية تعديل قد تصيب هذه البيانات (المادة 101).

تقترح النقابة تعديل المادة 99، لناحية مضمون المعلومات المتصلة بالبيانات الشخصية التي يمكن لصاحبها أو ورثته طلبها من المسؤول عن معالجة البيانات. ويسمح مشروع القانون لـ"كل صاحب صفة" أن يطلب، على سبيل المثال "معلومات تتعلق بالأشخاص الذين ترسل إليهم البيانات ذات الطابع الشخصي أو الذين يمكنهم الاطلاع عليها." وتشكل هذه المادة بابًا واسعًا للاطلاع على بيانات فئة كبيرة من الأفراد لمجرد الفضول. وهو ما يعني تشريع التعدي على خصوصية الأفراد. من هنا تقترح نقابة المحامين تعديل هذا البند ليصبح كالتالي: "لصاحب البيانات ذات الطابع الشخصي أو لأي من ورثته أن يطلب أيضًا من المسؤول عن معالجة البيانات ذات الطابع الشخصي وفق الشروط المحددة في الفقرة الثانية أعلاه، تسليمه المعلومات الإضافية التالية: غايات المعالجة، وفئاتها، ومصدرها، وموضوع المعالجة، وطبيعتها، وتحديد الأشخاص وفئاتهم الذين ترسل إليهم البيانات ذات الطابع الشخصي أو الذين يمكنهم الاطلاع عليها ومواقيتها وغايات هذا الاطلاع."

الفصل الخامس – أحكام جزائية

تتراوح العقوبات التي ينص عليها هذا الباب عن أفعال تؤدي إلى خرق سرية البيانات خارج الأطر القانونية، ما بين الغرامة المالية التي تصل إلى 15 مليون ليرة لبنانية والسجن الذي يصل الى 3 سنوات. التعديل الوحيد الذي تقترحه نقابة المحامين على هذا الباب هو تحديد المهلة التي يصبح من بعدها رفض المسؤول عن معالجة البيانات الشخصية عبارة عن جنحة. وهذه المهلة وفقًا لاقتراح النقابة يجب أن تكون 10 أيام. في حال استمر معالج البيانات بعد هذه المهلة برفض الإجابة على صاحب الطلب، يُعتبر هذا التصرف جنحة يعاقب عليها القانون بفرض غرامة تتراوح بين مليون و15 مليون ليرة لبنانية.

- **تقييم مشروع القانون على ضوء إرشادات الإسكوا**

ضمن إطار مشروع اللجنة الاقتصادية والاجتماعية لمنطقة غرب آسيا (الإسكوا)، وعنوانه "تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية"، وضعت الإسكوا لائحة من الإرشادات المتعلقة بالتشريع السيبراني. نتجت هذه الإرشادات عن بحث معمق يتناول مجموعة واسعة من التشريعات والاتفاقيات والدراسات في هذا المجال، لعلّ أهمها الاتفاقيات الدولية والإرشادات والتوصيات الصادرة عن الاتحاد الأوروبي، والقرارات الصادرة عن مجلس الأمم المتحدة والمجلس الأوروبي والاتحاد الدولي للاتصالات، بالإضافة إلى مجموعة من التشريعات العربية والأجنبية.[52]

تُظهر المقارنة بين مشروع القانون اللبناني وإرشادات الإسكوا الصادرة في بيروت تحديدًا، تفاوتًا بين الضمانات الواجب تأمينها لحماية بيانات الأشخاص وفقًا للإرشادات، وتلك المؤمنة في مشروع القانون. في البداية سنذكر بإيجاز أوجه التطابق بين الإرشادات ومشروع القانون، كونه سبق شرحها وهي:

- الحق في الاطلاع
- المعالجة الآمنة
- الالتزام بالفترة المحددة للمعالجة
- وجوب الإبلاغ والشفافية تجاه صاحب البيانات
- حق الوصول والتصحيح
- التصريح والترخيص: ربط إمكانية المعالجة بتقديم تصريح لجهة مختصة، على أن تكون إمكانية المعالجة بناء على تصريح هي الأصل، تُستثنى منها مجموعة من البيانات التي تحددها الدولة والتي تحتاج معالجتها للاستحصال على ترخيص
- ضمانة عدم إمكانية الاعتماد على البيانات المعالجة آلياً لاتخاذ أي قرار إداري أو قضائي في مواجهة صاحبها
- حظر معالجة بيانات الفرد المتعلقة بالحالة الصحية والهوية الوراثية والحياة الجنسية

إلا أن هذا الحظر يأتي مقتضبًا في نص مشروع القانون اللبناني، حيث تنص إرشادات الإسكوا على "حظر معالجة البيانات ذات الطابع الشخصي التي تكشف عن الأصل العرقي أو الاثني، وعن الآراء السياسية أو الدينية أو الفلسفية، وعن الانتماء النقابي، كذلك معالجة البيانات المتعلقة بصحة الإنسان وبحياته الجنسية."

تتضمن كل من إرشادات الإسكوا ومشروع القانون اللبناني استثناءات على الحظر. نظريًا، قد تبدو الاستثناءات اللبنانية أقل، ما يكفل

بالتالي تطبيقًا أوسع للحظر. لكن عمليًا، لا بد من تسجيل حذر من الاستثناء الذي يسمح بإجراء المعالجة بناء على ترخيص صادر عن وزير الصحة العامة (أي وفقًا لأحكام المادة 97). بالتالي يشكل هذا الاستثناء بابًا لتوسيع إطار الحظر، وحتى القضاء عليه. بالمقابل تخلو إرشادات الإسكوا من أي نص نظير لهذا الاستثناء.

• المبادئ المشار إليها في إرشادات الإسكوا

خلافًا لإرشادات الإسكوا، لا يعدّد القانون الحالات التي تُسمح فيها معالجة البيانات الشخصية. ففيما يُظهر مشروع القانون اللبناني اتجاهًا نحو اعتبار أن معالجة البيانات هي حرة في الأصل، ولا تتطلب إلا التقدم بتصريح أمام وزارة الاقتصاد باستثناء حالات محددة تتطلّب ترخيصًا. بالمقابل تبدو إرشادات الإسكوا واضحة من حيث أن معالجة البيانات الشخصية لا يمكن أن تخضع لمبدأ "الحرية هي الأصل"، بل يجب أن تكون مقيدة كونها تتعلق بحياة الآخرين الشخصية. لذا تشير الإرشادات إلى أنه "لا يمكن جمع البيانات ذات الطابع الشخصي إلا في الحالات التالية: إعطاء الشخص المعني موافقته أو أن تكون المعالجة ضرورية لتنفيذ عقد تكون فيه معالجة البيانات ضرورية أو إذا كانت معالجة البيانات ضرورية لاحترام التزام قانون ملقى على عاتق مراقب المعالجة أو ضرورية لصيانة مصلحة حيوية للشخص المعني أو ضرورية لتنفيذ مهمة متعلقة بالمصلحة العامة أو تدخل ضمن ممارسة السلطة العامة من قبل مراقب المراجعة أو من قبل الغير المرسلة إليه البيانات أو إذا كانت ضرورية لتحقيق المصلحة المشروعة لمراقب المعالجة أو للغير المرسلة إليه البيانات."

• نقل البيانات الشخصية إلى دولة أجنبية

يغيب عن مشروع القانون اللبناني أي ذكر لمبدأ عدم جواز نقل البيانات الشخصية موضوع المعالجة إلى بلد أجنبي. هذا المبدأ الذي تكرسه الإسكوا، معلقةً اياه على شرط توفير البلد الأجنبي مستوى ملائم من الحماية القانونية، حيث يصبح نقل البيانات ممكنًا. وتُسجل لهذه الناحية مخاوف عديدة من إغفال هذا البند في مشروع القانون اللبناني، لا سيما لناحية كونه بلد لجوء للعديد من الأشخاص الفارين من أنظمة ديكتاتورية، ومن نزاعات وحروب. بالإضافة إلى كونه ملتزمًا باتفاقيات تلزمه تقديم بيانات شخصية عن الأفراد إلى دول هؤلاء. فعلى سبيل المثال لبنان عضو في الاتفاقية العربية لمكافحة الإرهاب الموقعة في القاهرة في 222 نيسان/أبريل 1998، وقد صادق عليها بموجب القانون رقم 57 المؤرخ في 31 آذار/مارس 1999. وتتعهد كل من الدول المتعاقدة، بتزويد أي دولة متعاقدة أخرى، بما يتوافر لديها من معلومات أو بيانات من شأنها أن تساهم في مكافحة الإرهاب، ومن بين البيانات التي يمكن تبادلها "أوصاف الشخص المطلوب تسليمه بأكبر قدر ممكن من الدقة، وأي بيانات أخرى من شأنها تحديد شخصه وجنسيته وهويته". والحال أن الهدف من هذه الاتفاقية هو سامٍ بالمبدأ، غير أن التطبيقات المتعسفة لقوانين الإرهاب وكيفية استخدامها في انتهاك حقوق الإنسان في العديد من الدول العربية، يؤدي إلى القول أن هذه الاتفاقية تفتح بابًا كبيرًا لانتهاك بيانات كل مقيم في لبنان، وتعريضه للخطر في دولته، ما دام التشريع اللبناني خالٍ من أي تنظيم يحمي البيانات الشخصية.

• هيئة المراقبة

تضمنت المسودة الأولى لمشروع قانون المعاملات الإلكترونية وحماية البيانات الشخصية أحكامًا منشئة لهيئة مستقلة تُعنى بمراقبة تنفيذه والالتزام بأحكامه. غير أن هذه المواد قد تم حذفها، ولا يتضمن المشروع الحالي أي ذكر لهيئة مماثلة. إلى ذلك، تتضمن إرشادات الإسكوا بندًا يتعلق بضرورة أن تنص القوانين السيبرانية على إنشاء "هيئة رقابة رسمية مختصة". وتكون وظيفة الهيئة بشكل أساسي مراقبة حسن تطبيق أحكام الإرشاد وتمارس مهامها بشكل مستقل.

تشمل صلاحيات هذه الهيئة:

- تلقي تصاريح معالجة البيانات الشخصية ومنح التراخيص
- صلاحية التحقيق مثل الوصول إلى البيانات وجمع المعلومات بهدف القيام بدورها في الرقابة
- التدخل وفرض عقوبات إدارية مثل منع القيام بعملية معالجة أو الأمر بمنع الدخول أو محو أو تدمير بيانات ما
- المثول أمام القضاء في حال مخالفة مضمون الإرشاد
- تقديم استشارات أو اقتراحات لتطوير النصوص القانونية
- التعاون مع الهيئات الأجنبية المختصة في مجال البيانات الشخصية

الخاتمة

إن النص بصيغته الحالية وحتى بعد المناقشات المطوّلة في اللجان النيابية تعتريه الكثير من نقاط الضعف التي تجعل منه دون أية فائدة عملية. فبالرغم من أن قواعده آمرة وهي ليست محصورة بالمعالجات الآلية والالكترونية فقط للبيانات إلا أن الاستثناءات الكثيرة تضيّق من هامش حماية البيانات ذات الطابع الشخصي (مواد 87، 91، 92، 94، 103 على سبيل المثال).

كما وان هذا المشروع ينص على أن من يعطي التراخيص ويتلقى التصاريح بتجميع ومعالجة البيانات هو وزارة الاقتصاد والتجارة أي السلطة التنفيذية، وهي نقطة ضعف أُخرى لأن من يؤتمن على مراقبة واحترام الحياة الخاصة والحريات العامة هو السلطة القضائية لا التنفيذية. إن التوفيق بين مبادئ الحرية والأمان كما والتوازن بين الحق بالوصول للمعلومات العامة والحق بحماية الخصوصية والبيانات ذات الطابع الشخصي لا يمكن أن يتم بصورة ناجعة إلا من خلال إنشاء هيئة إدارية مستقلة.

وفي حال تعذر ذلك من الممكن إناطة هذه المهمة بصورة مؤقتة إلى لجنة حل النزاعات المنصوص عنها في القانون رقم 659 الصادر في 4 شباط 2005 وتعديلاته (قانون حماية المستهلك) وذلك بعد تعديل نص المادة 97 (تأليف اللجنة) كما وتعديل المادة 98 (اختصاص اللجنة) لكي يشمل إعلام الأشخاص المعنيين والمسؤولين عن معالجة البيانات الشخصية حقوقهم والتزاماتهم، وضمان أن معالجة البيانات الشخصية تمتثل للمبادئ والقواعد المنصوص عنها في مشروع القانون 9341 كما واناطة صلاحية إعطاء الترخيص وتلقي التصاريح لمعالجة البيانات بها.

إقتباسات

[1] دعوة لتقديم الطلبات: منحة زمالة لإعداد التقارير عن الحريات الرقمية. (2017، يناير SMEX(2. استرجع من http://bit.ly/2urgtBq

[2] رسم خريطة المراقبة الرقمية الجماعية في لبنان. (2017، فبراير 9). SMEX. استرجع من http://bit.ly/2hIVmJ0

[3] تجدر الإشارة إلى أن القانون 140 قد صدر في ظروف كانت فيها سبل اعتراض خصوصية الأفراد وبياناتهم الشخصية غير مضبوطة وغير خاضعة لأي نصوص قانونية وتنظيمية حيث كانت الحماية المقر بها دستوريًا غير متوافرة فعليًا وكان أي شخص معرضًا للتدخل في خصوصية حياته الشخصية وخرق سرية بياناته الشخصية. هذا وقد استلهم المشرع اللبناني عند إقراره القانون، نصًا وروحًا، من القانون الفرنسي رقم 646/1991 إلا أن عدم إصدار المراسيم التنظيمية لتطبيق هذا القانون بالسرعة اللازمة وعدم مباشرة الهيئة المستقلة المناط بها التثبت من قانونية طلبات الاعتراض الإداري على المخابرات الهاتفية، عملها قبل العام 2011 أديا إلى الحد من فعالية القانون المذكور كما سنبين في صلب هذه الدراسة.

[4] التعريف وفقًا للقانون الفرنسي:

Article 2, loi n 2004-801 du 6 août 2004: Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.

[5] لجنة الأمم المتحدة الاقتصادية والاجتماعية لغرب آسيا (إسكوا). (2012). إرشادات الإسكوا للتشريعات السيبرانية، مشروع تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية. استرجع من
https://www.unescwa.org/sites/www.unescwa.org/files/page_attachments/directives-full.pdf

[6] التعريف وفقًا للقانون الفرنسي:

Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

[7] برجس، ا. (2017). بعد 11 سنة من إنشائها، محكمة المستهلك تباشر عملها. المفكرة القانونية، (48). استرجع من
http://www.legal-agenda.com/article.php?id=3602

[8] قانون رقم 140/1999

[9] قانون رقم 431/2002، المادة 38

[10] تقرير حول الحق بالخصوصية في لبنان، أعدته كل من منظمة SMEX، والخصوصية الدولية، وجمعية الاتصالات التقدمية خلال الاستعراض الدوري الشامل لعام 2016، إسترجع من https://goo.gl/K4P7tC

[11] المؤتمر الثاني للمتخصّصين في أمن وسلامة الفضاء السيبراني (الإنترنت). المركز العربي للبحوث القانونية والقضائية جامعة الدول العربية - مجلس وزراء العدل العرب. (د.ت). استرجع من http://bit.ly/2wtKt14

[12] الاتفاقية العربية لمكافحة الإرهاب الموقعة في القاهرة في 222 نيسان 1998، ومن بين الدول التي انضمت إليها أيضاَ، إجازة الإبرام ومضمون الاتفاقية استرجع من http://www.madcour.com/LawsDocuments/LDOC-44-635278203054882024.pdf

[13] في هذا المجال يمكن مراجعة: سارة رمال، الحق في الخصوصية في العصر الرقمي (قراءة تحليلية في ضوء قرار الجمعية العامة رقم 68/167)، رسالة ماجستير، الصفحات 62 وما يليها (2016)

[14] Rouse, M. (2015, November). O-code/low-code app development evolves from loathed to loved, Essential Guide, biometrics. Retrieved from http://searchsecurity.techtarget.com/definition/biometrics

[15, 16, 17, 18] Information Commissioner RS. (2008, February). Guidelines for the introduction of biometric measures. Retrieved from https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Guidelines_Biometrics.pdf

[19] No-code/low-code app development evolves from loathed to loved. (n.d.). Retrieved from http://searchsecurity.techtarget.com/definition/encryption

[20] خبير في أمن المعلومات، رئيس قسم تكنولوجيا المعلومات والتواصل في الجامعة الأمريكية للعلوم والتكنولوجيا

[21] بيان صادر عن المديرية العامة للأمن العام. المديرية العامة للأمن العام اللبناني. (2017). استرجع من http://www.general-security.gov.lb/ar/posts/221

[22] بطاقة الإقامة البيومترية الذكية. المديرية العامة للأمن العام اللبناني. (2014). استرجع من http://www.general-security.gov.lb/ar/posts/60

[23] المباشرة بإصدار جوازات السفر اللبنانية البيومترية. المديرية العامة للأمن العام اللبناني. (2016). استرجع من
http://www.general-security.gov.lb/ar/posts/182

[24] كتاب موجه من المديرية العامة للأمن العام إلى منظمة SMEX في 26 أيار/مايو 2017

[25] الشوفي، إ. (2016، يناير 8). تجديد جوازات السفر: الرسوم تُسدد مرتين. جريدة الأخبار. استرجع من http://www.al-akhbar.com/node/249438

[26] الشوفي، إ. (2016، يناير 9). 200 ألف جواز سفر «خارج الخدمة». جريدة الأخبار. استرجع من http://www.al-akhbar.com/node/249546

[27] منذر، ر. (2016، يناير 9). الأمن العام يوضح مسألة استبدال الجوازات. جريدة الجمهورية. استرجع من
http://www.aljoumhouria.com/news/index/283847

[29, 28] عقيل، ر. (2016). جواز السفر... بكلّ ثقة. مجلة الأمن العام، (29). استرجع من
http://www.general-security.gov.lb/ar/magazines/magazine/42

[30] بلوط، م. (2016، يونيو 20). هذه قصة جواز السفر «البيومتري».. وآلية هبة المليار دولار. جريدة السفير. استرجع من
http://assafir.com/Article/426382

[31] موقع شركة جيمالتو. (د.ت).

[32] موقع شركة انكربت. (د.ت).

[33] Neal, D. (2015, February 25). Gemalto: It looks like we were hacked by GCHQ and NSA. Retrieved from
https://www.theinquirer.net/inquirer/news/2396223/sim-card-security-scare-gemalto-is-investigatiing-uk-and-us-hack-allegations

[34, 35] ISO/IEC 19794-7:2014. (2014). Retrieved from https://www.iso.org/standard/55938.html

[38, 37, 36] الديراني، ز. (2013، مايو 28). إدارة «الأميركية» تتجسس على أهلها. جريدة الأخبار. استرجع من http://www.al-akhbar.com/node/183870

[39] AUB Leaks. (n.d.). Retrieved from http://aubleaks.wordpress.com

[40] مهدي، ح. (2014، ديسمبر 9). سابقة قضائية في قضية AUB ليكس: تكريس مبدأ سموّ المصلحة العامة. جريدة الأخبار. استرجع من
http://al-akhbar.com/node/221518

[41] حاوي، ز. (2016، فبراير 4). حسين مهدي «فاشي الأسرار» مثلَ أمام القضاء. جريدة الأخبار. استرجع من http://www.al-akhbar.com/node/251352

[42] Alfa Website. (n.d.). Description of service. Alfa Media. Retrieved from https://www.alfa.com.lb/media/sms.aspx?language=1&cat=1&subcat=1

[43] Touch website. (n.d.). SMS Advertising. Mobile Media. Retrieved from
https://www.touch.com.lb/autoforms/portal/touch/business/sms-advertising/mobile-media

[44] مصيبة في لبنان... انتهاكات واعتداءات. (2013، آذار/مارس 14). صدى صيدا. استرجع من http://www.sadasaida.com/news.php?go=fullnews&newsid=29853

[45] أحد مُعدي هذا التقرير (حسين مهدي) كان ضمن مُعدي التحقيق وقد اطلع على هذه البيانات غير المحمية وغير المشفرة

[46] رالي الجمارك: سباق التهرب الضريبي - رياض قبيسي. (2017). استرجع من https://www.youtube.com/watch?v=DLgu0v4RaN4

[48, 47] المقدم، ن. (2010، فبراير 23). تزوير لوحات السيارات: عصابات تنتفع من النافعة. جريدة الأخبار. استرجع من http://al-akhbar.com/node/58400

[49] طانيوس، ك. (2015، فبراير 25). فضيحة جديدة: لوحة سيارتك باتت تعرض تفاصيل حياتك! جريدة النهار. استرجع من http://bit.ly/2upL71S

[50] مخلوف، ي. (2011، سبتمبر 26). مشروع قانون تنظيم المعاملات الالكترونية: التمايز في إعلان مبدأ "احترام الخصوصية" والتمايز في نسفه. المفكرة القانونية. استرجع من
http://www.legal-agenda.com/article.php?id=31

[51] الموقع الرسمي لمجلس النواب، نشاطات نيابية 1/12/2011. استرجع من https://goo.gl/HrC1Qn

[52] إرشادات الإسكوا للتشريع السيبراني، الصادر في بيروت عام 2012، ص د.

السّيرة الذاتية للكتّاب

إلهام برجس صحافية وباحثة قانونية تقوم بتوثيق وإعداد تقارير عن العمليات القضائية والإجراءات القانونية، بغية النهوض بحقوق الإنسان في لبنان. تعمل إلهام حاليًا على تحضير أطروحة الماجستير حول القانون الدستوري. كما تم نشر كتاباتها في العديد من الصحف، أبرزها المدن والديار والأخبار.

حسين مهدي صحافي يتمتع بخبرة واسعة في مجالات الصحافة المطبوعة والإذاعة ووسائط الإعلام الرقمية. عمل حسين على كشف النقاب عن الفساد المستشري وجرائم الاحتيال المتربصة بالعديد من جامعات لبنان المشهورة، من بينها الجامعة الأميركية في بيروت والجامعة اللبنانية. كونه مدافع قوي عن حريات الصحافة، وبالرغم من وابل الدعاوى القضائية المرفوعة ضده والتهديدات الهادفة إلى إخافته وطمس صوته، فإن حسين يواصل عمله على قدم وساق.

سارة رمال حائزة على شهادة ماجستير في القانون العام من الجامعة اللبنانية ودبلوم في القانون الدولي من جامعة آدم ميكيويكز في بوزنان في بولندا. هي كاتبة "الحق في الخصوصية في العصر الرقمي: قراءة تحليلية في ضوء قرار الجمعية العامة للأمم المتحدة 68/167."

الدكتور بيار الخوري خبير قانوني في مجال تكنولوجيا المعلومات والاتصالات وحماية المستهلك. وهو يدرّس القانون التجاري، والعقود، والشركات، والملكية الفكرية وقوانين التكنولوجيا الاتصالات والمعلومات. بالإضافة إلى التدريس، فهو محام في نقابة المحامين في بيروت متخصص في قوانين الملكية الفكرية وتكنولوجيا الاتصالات والمعلومات. يشغل منصب الرئيس القانوني للمشاع الإبداعي Creative Commons في لبنان، وهو عضو في اللجنة النيابية الفرعية المنبثقة عن اللجان المشتركة التي تدرس حالياً مشروع قانون المعاملات الالكترونية والبيانات ذات الطابع الشخصي في المجلس النيابي.


SMEX